ALGEBRA AND NUMBER THEORY: Solutions

Michaelmas term 2009

1. (i) Yes. (ii) No (the odd integers don't form an additive group: $+$ is no operation, since "odd+odd=even"; also there is no zero element). (iii) No (there is no additive inverse). (iv) Yes. (v) No ($\cdot$ is no operation, since e.g. multiplying the element $x = x^1$ with itself gives an even power of x). (vi) No (the zero element would have to be the constant function 0, but this is continuous). (vii) No (any non-zero function from $[0,1]$ to $[0,\infty]$ is lacking an additive inverse which would have to map to $[0,-\infty]$).

2. We certainly already know $\mathbf{Z}_n$ is an abelian group under addition, with neutral element $\overline{0}$, and the inverse of $\overline{a}$ given by $\overline{-a}$. To check the remaining two axioms, let $\overline{a}$, $\overline{b}$ and $\overline{c}$ be in $\mathbf{Z}_n$. Then $(\overline{a}\,\overline{b})\,\overline{c} = \overline{ab}\,\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\,\overline{bc} = \overline{a}\,(\overline{b}\,\overline{c})$ where we used associativity in $\mathbf{Z}$. Distributivity in $\mathbf{Z}_n$ reduces to the distributivity in $\mathbf{Z}$ in a similar way.

3. We use that two functions on X are the same if and only if they have the same value for all elements in X. So, e.g., in order to check that $(f+g)h = fh + gh$, we compare the values of both sides for any $x \in X$. Now $[(f+g)h](x) = [f+g](x) \cdot h(x) = (f(x)+g(x))h(x) = f(x)h(x) + g(x)h(x)$ because $\mathbf{Z}$ is a ring. $[fh+gh](x) = [fh](x) + [gh](x) = f(x)h(x) + g(x)h(x)$, so that indeed $(f+g)h = fh + gh$. The rest of the verifications are similar, with the zero element given by the zero function $x \mapsto 0$, the inverse of $f : x \mapsto f(x)$ given by $g : x \mapsto -f(x)$. This ring has an identity as well: the function given by $x \mapsto 1$.

4. In $\mathbf{Z}_6$, the elements $\overline{a}$ with $\overline{a}^2 = \overline{a}$ are $\{\overline{0}, \overline{1}, \overline{3}, \overline{4}\}$, so there are two here we can use. We could also take $R = \mathbf{Z} \times \mathbf{Z}$, a direct product of rings. Then $(1,0)^2 = (1,0)$. Note that $(1,0)$ is *not* the identity of $\mathbf{Z} \times \mathbf{Z}$, which is $(1,1)$.

Another possibility: take $R = M_2(\mathbf{Z})$. Then $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, but the identity of R is the 2×2 identity matrix.

Yet another possibility is, for any integer $n > 1$, the $(n \times n)$-matrix (a_{ij}) with all entries $a_{ij} = 1/n$.

5. By assumption, for any r in R, $r + r = (r+r)^2 = r(r+r) + r(r+r) = r^2 + r^2 + r^2 + r^2 = r + r + r + r$. Adding $-r - r$ we get $r + r = 0$. If s is also an element of R, then $r + s = (r+s)^2 = r(r+s) + s(r+s) = r^2 + rs + sr + s^2 = r + rs + sr + s$, from which we get that $rs + sr = 0$. Adding rs on both sides yields $sr = rs$ as $rs + rs = 0$. Examples of such rings are $\left(\mathbf{Z}_2\right)^n = \underbrace{\mathbf{Z}_2 \times \ldots \times \mathbf{Z}_2}_{n}$ for any n.

6. The set $R[[X]]$ is closed under addition and multiplication which follows immediately from the formulas for them; in other words, they are in fact *operations*, as requested.

We first show that $R[[X]]$ is an abelian group under addition, with neutral element $0_{R[[X]]} = \sum_i 0_R X^i$. If $\alpha = \sum_i a_i X^i$, $\beta = \sum_i b_i X^i$ and $\gamma = \sum_i c_i X^i$ are elements in $R[[X]]$, then $(\alpha+\beta)+\gamma = \left(\sum_i (a_i + b_i) X^i\right) + \sum_i c_i X^i = \sum_i ((a_i + b_i) + c_i) X^i = \sum_i (a_i + (b_i + c_i)) X^i = \sum_i a_i X^i + \sum_i (b_i + c_i) X^i = \alpha + (\beta + \gamma)$ because addition in R is associative. Because $r + 0_R = r$ for any r in R, we find that $\alpha + \sum_i 0_R X^i = \sum_i (a_i + 0_R) X^i = \sum_i a_i X^i = \alpha$, and similarly $\sum_i 0_R X^i + \alpha = \alpha$. Because R is an abelian group under addition, the element $\delta = \sum_i (-a_i) X^i$ exists, and $\alpha + \delta = \alpha + \sum_i (-a_i) X^i = \sum_i (a_i + (-a_i)) X^i = \sum_i 0_R X^i = 0_{R[[X]]}$, and similarly $\delta + \alpha = 0_{R[[X]]}$. Finally, because addition in R is commutative, we find that $\alpha + \beta = \sum_i (a_i + b_i) X^i = \sum_i (b_i + a_i) X^i = \beta + \alpha$. Distributivity in $R[[X]]$ follows similarly from the properties of R: $\alpha(\beta + \gamma) = \left(\sum_i a_i X^i\right)\left(\sum_i (b_i + c_i) X^i\right) = \sum_i \left(\sum_{j=0}^i a_j (b_{i-j} + c_{i-j})\right) X^i = \sum_i \left(\sum_{j=0}^i (a_j b_{i-j} + a_j c_{i-j})\right) X^i = \left(\sum_i \left(\sum_{j=0}^i a_j b_{i-j}\right) X^i\right) + \left(\sum_i \left(\sum_{j=0}^i a_j c_{i-j}\right) X^i\right) = \alpha\beta + \alpha\gamma$. Similarly $(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$. Finally, for the associativity of the multiplication, $(\alpha\beta)\gamma = \left(\sum_i \left(\sum_{j=0}^i a_j b_{i-j}\right) X^i\right)\gamma = \sum_i \left(\sum_{j'=0}^i \left(\sum_{j=0}^{j'} a_j b_{j'-j}\right) c_{i-j'}\right) X^i$ because we have to replace i with j everywhere in the expression for $\alpha\beta$, but j has already been used as summation index. Because multiplication in R is associative, we do not

have to write parentheses, and the expression equals $\sum_i \left(\sum_{\substack{j_1+j_2+j_3=i \\ j_1,j_2,j_3 \geq 0}} a_{j_1} b_{j_2} c_{j_3} \right) X^i$. Starting with $\alpha(\beta\gamma)$ gives exactly the same result, so that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

The formulas for addition and multiplication in $R[X]$ are the same as for $R[[X]]$, so that we only have to check that it is a subring. Clearly $0_{R[[X]]}$ has only finitely many nonzero coefficients (namely none), and if α and β have only finitely many nonzero coefficients, then $\alpha - \beta$ and $\alpha\beta$ have only finitely many nonzero coefficients as well.

7. We check the conditions for a subring. We already know that $\varphi(0_R) = 0_S$ by the theory of group homomorphisms (recall φ is in particular a homomorphism of groups with respect to the addition). If a and b are in the image, say $\varphi(r) = a$ and $\varphi(s) = b$, then $a - b = \varphi(r) - \varphi(s) = \varphi(r - s)$ and $ab = \varphi(r)\varphi(s) = \varphi(rs)$ are both in the image of φ.

8. We have to show that for every s in S, $\varphi(1_R)s = s\varphi(1_R) = s$. $s = \varphi(r)$ for some r in R as φ is surjective, so $s\varphi(1_R) = \varphi(r)\varphi(1_R) = \varphi(r \cdot 1_R) = \varphi(r) = s$. Similarly $\varphi(1_R)s = s$.

9.

(i) We know this from group theory, as φ is a homomorphism of groups with respect to addition, so φ must preserve inverses.

(ii) Elements in $\varphi(R)$ are of the form $\varphi(r)$ for some r in R. So if we have two such elements, $\varphi(r_1)$ and $\varphi(r_2)$, then $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) = \varphi(r_2 r_1) = \varphi(r_2)\varphi(r_1)$. It does not follow that S is commutative (unless, e.g., φ is surjective). For example, $\varphi : \mathbf{R} \to M_2(\mathbf{R})$ mapping a to $\left(\begin{smallmatrix} a & o \\ 0 & a \end{smallmatrix}\right)$ is a homomorphism of rings, and $\mathbf{R}$ is commutative, but $M_2(\mathbf{R})$ is not.

(iii) Since A is a subring of R, it contains 0_R, so $\varphi(A)$ in S contains $\varphi(0_R) = 0_S$. Let s and t be in $\varphi(A)$. We have to check that $s - t$ and st are in $\varphi(A)$. We must have $s = \varphi(a)$ and $t = \varphi(b)$ for some a and b in A as s and t are in $\varphi(A)$. Then $s - t = \varphi(a) - \varphi(b) = \varphi(a - b)$ and $st = \varphi(a)\varphi(b) = \varphi(ab)$. Both lie in $\varphi(A)$ as A is a subring of R, so $a - b$ and ab lie in A as a and b are in A.
This completes the check of the conditions for a subring (of S).

10. The first two are ring homomorphisms (they are special cases of the "specialisation homomorphism" in the lectures). For the third, let $f(X) = \sum_i a_i X^i$ and $g(X) = \sum_i b_i X^i$ be in $\mathbf{Z}[X]$. Then $\varphi(f(X) + g(X)) = \varphi(\sum_i (a_i + b_i) X^i) = \sum_i (a_i + b_i)(-X)^i = \sum_i a_i (-X)^i + \sum_i b_i (-X)^i = \varphi(f(X) + \varphi(g(X))$, and $\varphi(f(X)g(X)) = \varphi(\sum_i \left(\sum_{j=0}^{i} a_i b_{i-j} \right) X^i) = \sum_i \left(\sum_{j=0}^{i} a_i b_{i-j} \right) (-X)^i = \left(\sum_i a_i (-X)^i \right) \left(\sum_i b_i (-X)^i \right) = \varphi(f(X))\varphi(g(X))$ by collecting equal powers of $-X$. So φ is a homomorphism of rings in this case. (This would also be true if we took any $h(X)$ in $\mathbf{Z}[X]$ instead of $-X$, again using some specialisation homomorphism, with $S = \mathbf{Z}$, $R = \mathbf{Z}[X]$ and $a = h(X)$.) The last is not a homomorphism of rings as it does not preserve addition, e.g., $\varphi(X + 1) = 3^2 \neq 5 = \varphi(X) + \varphi(1)$.

11.

(i) Clearly $0 = \frac{0}{1}$ is in R. If a/b and c/d are in R, we can assume $\mathbf{gcd}(n, b) = \mathbf{gcd}(n, d) = 1$. Then $\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$ and $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ are in R as $\mathbf{gcd}(n, bd) = 1$ as well. Finally, $1 = \frac{1}{1}$ is in R, which is the identity.

(ii) Note the map makes sense, as $\mathbf{gcd}(n, b) = 1$, so $\overline{b}$ is in $\mathbf{Z}_n^*$, and $\left(\overline{b}\right)^{-1}$ makes sense. If $\frac{a}{b} = \frac{c}{d}$ with $\mathbf{gcd}(n, b) = \mathbf{gcd}(n, d) = 1$, $ad = bc$. So in $\mathbf{Z}_n$, $\overline{ad} = \overline{bc}$ and $\overline{a}\left(\overline{b}\right)^{-1} = \overline{c}\left(\overline{d}\right)^{-1}$, so using either $\frac{a}{b}$ or $\frac{c}{d}$ gives the same value for φ on this element. φ is surjective because $0, 1, \ldots, n-1$ are in R and they map to $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. To check φ is a homomorphism of rings, let $\frac{a}{b}$ and $\frac{c}{d}$ be in R. Then $\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{ad+bc}{bd}) = \overline{ad + bc}\left(\overline{bd}\right)^{-1} = \overline{a}\left(\overline{b}\right)^{-1} + \overline{c}\left(\overline{d}\right)^{-1} = \varphi(\frac{a}{b}) + \varphi(\frac{c}{d})$. Also $\varphi(\frac{a}{b}\frac{c}{d}) = \varphi(\frac{ac}{bd}) = \overline{ac}\left(\overline{bd}\right)^{-1} = \overline{a}\left(\overline{b}\right)^{-1}\overline{c}\left(\overline{d}\right)^{-1} = \varphi(\frac{a}{b})\varphi(\frac{c}{d})$. For the kernel, $\overline{a}\left(\overline{b}\right)^{-1} = \overline{0}$ if and only if $\overline{a} = \overline{0}$, so the kernel consist of the elements of the form a/b with $n|a$ and $\mathbf{gcd}(n, b) = 1$.

12.

(i) We check the conditions on a subring. Clearly $0 = 0 + 0 \cdot \sqrt{D}$ is in $\mathbf{Z}[\sqrt{D}]$, and if $a + b\sqrt{D}$ and $c + d\sqrt{D}$ are in $\mathbf{Z}[\sqrt{D}]$, so a, b, c and d are in $\mathbf{Z}$, then $(a + b\sqrt{D}) - (c + d\sqrt{D}) = (a - c) + (b - d)\sqrt{D}$

and $(a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD)+(ad+bc)\sqrt{D}$ are in $\mathbf{Z}[\sqrt{D}]$ because $a-c$, $b-d$, $ac+bdD$ and $ad+bc$ are in $\mathbf{Z}$. (The fact that D is not a square in $\mathbf{Z}$ is not used, but it does mean that in $\mathbf{Z}[\sqrt{D}]$, $a+b\sqrt{D} = c+d\sqrt{D}$ if and only if $a=c$ and $b=d$.) If $\alpha = a+b\sqrt{D}$ and $\beta = c+d\sqrt{D}$, $\alpha\beta = (ac+bdD)+(ad+bc)\sqrt{D}$, so $N(\alpha\beta) = (ac+bdD)^2-(ad+bc)^2D = a^2c^2+b^2d^2D^2-a^2d^2D-b^2c^2D = (a^2-b^2D)(c^2-d^2D) = N(\alpha)N(\beta)$. N is not a homomorphism of rings as it does not preserve addition. E.g., $N(1+1) = 4 \neq 2 = N(1)+N(1)$.

(ii) This is completely analogous to (i).

13. We first show that $\varphi : \mathbf{Z}[\sqrt{D}] \to \mathbf{Z}[\sqrt{D}]$ given by mapping $a+b\sqrt{D}$ to $a-b\sqrt{D}$ is a homomorphism of rings. Let $a+b\sqrt{D}$ and $c+d\sqrt{D}$ be in $\mathbf{Z}[\sqrt{D}]$. Then $\varphi((a+b\sqrt{D})+(c+d\sqrt{D})) = \varphi((a+c)+(b+d)\sqrt{D}) = (a+c)-(b+d)\sqrt{D} = \varphi(a+b\sqrt{D})+\varphi(c+d\sqrt{D})$, and $\varphi((a+b\sqrt{D})(c+d\sqrt{D})) = \varphi((ac+bdD)+(ad+bc)\sqrt{D}) = (ac+bdD)-(ad+bc)\sqrt{D} = (a-b\sqrt{D})(c-d\sqrt{D}) = \varphi(a+b\sqrt{D})\varphi(c+d\sqrt{D})$, so that φ is indeed a homomorphism of rings. Because clearly $\varphi^2 : \mathbf{Z}[\sqrt{D}] \to \mathbf{Z}[\sqrt{D}]$ is the identity map, φ must also be injective and surjective, so it is an isomorphism of rings.

14. Let $\psi : R[X] \to S[X]$ be the indicated map. Let $f(X) = \sum_i a_i X^i$ and $g(X) = \sum_i b_i X^i$ be elements of $R[X]$. Then $\psi(f(X)+g(X)) = \psi(\sum_i (a_i+b_i)X^i) = \sum_i \varphi(a_i+b_i)X^i = \sum_i (\varphi(a_i)+\varphi(b_i))X^i = \left(\sum_i \varphi(a_i)X^i\right) + \left(\sum_i \varphi(b_i)X^i\right) = \psi(f(X)) + \psi(g(X))$, and for the product we find

$$\psi(f(X)g(X)) = \psi\left(\sum_i \left(\sum_{j=0}^{i} a_j b_{j-i}\right) X^i\right) = \sum_i \varphi\left(\sum_{j=0}^{i} a_j b_{j-i}\right) X^i = \sum_i \left(\sum_{j=0}^{i} \varphi(a_j b_{j-i})\right) X^i =$$
$$= \sum_i \left(\sum_{j=0}^{i} \varphi(a_j)\varphi(b_{j-i})\right) X^i = \left(\sum_i \varphi(a_i)X^i\right)\left(\sum_i \varphi(b_i)X^i\right) = \psi(f(X))\psi(g(X)).$$

15.

(i) Let $\alpha = a+bi$ and $\beta = c+di$ be in $\mathbf{Z}[i]$. Then $\varphi(\alpha+\beta) = \varphi((a+b)+(c+d)i) = \overline{(a+b)+2(c+d)} = \overline{a+2c} + \overline{a+2d} = \varphi(\alpha)+\varphi(\beta)$, and $\varphi(\alpha\beta) = \varphi((a+b)(c+d)i) = \varphi((ac-bd)+(ad+dc)i) = \overline{(ac-bd)+2(ad+dc)} = \overline{ac+4bd+2ad+2dc} = \overline{(a+2b)(c+2d)} = \overline{a+2b}\,\overline{c+2d} == \varphi(\alpha)\varphi(\beta)$.

(ii) $\varphi((5k-2b)+bi) = \overline{5k-2b+2b} = \overline{5k} = \overline{0}$. If $a+bi$ is such that $\varphi(a+bi) = \overline{a+2b} = \overline{0}$, then $a+2b = 5k$ for some k in $\mathbf{Z}$. Then $a = 5k-2b$, so $a+bi = (5k-2b)+bi$.

(iii) That $5 = (-2+i)(-2-i)$ is simple to compute. Applying φ to $(c+di)(-2+i)$, we find $\varphi((c+di)(-2+i)) = \varphi(c+di)\varphi(-2+i) = \varphi(c+di)\overline{0} = \overline{0}$. If $\varphi(a+bi) = \overline{0}$, then it is of the form $(5k-2b)+bi$ by the previous part. Then $a+bi = (5k-2b)+bi = (-2+i)(-2-i)k + b(-2+i) = (k(-2-i)+b)(-2+i) = (b-2k-ki)(-2+i)$ is of the required shape.

16. $\varphi(1_R) = \varphi(1_R^2) = \varphi(1_R)^2$, so $\varphi(1_R)(\varphi(1_R)-1_S) = 0$. Because S is an integral domain, it follows that either $\varphi(1_R) = 0_S$, or $\varphi(1_R) = 1_S$. If $\varphi(1_R) = 0_S$, then for r in R, $\varphi(r) = \varphi(r\cdot 1_R) = \varphi(r)\varphi(1_R) = \varphi(r)0_S = 0_S$.

17. If φ is such a ring homomorphism, then $\varphi(1) = \varphi(1^2) = \varphi(1)^2$. There are only two solutions to the equation $X^2 = X$ in $\mathbf{Z}_5$: $\overline{0}$ and $\overline{1}$ because $\mathbf{Z}_5$ is a field. If $\varphi(1) = \overline{1}$, then $\varphi(\sqrt{2})^2 = \varphi(\sqrt{2}^2) = \varphi(1+1) = \overline{1}+\overline{1} = \overline{2}$. But $X^2 = \overline{2}$ has no solutions in $\mathbf{Z}_5$, so this cannot happen. Therefore $\varphi(1) = \overline{0}$, and $\varphi(\alpha) = \varphi(\alpha\cdot 1) = \varphi(\alpha)\varphi(1) = \varphi(\alpha)\overline{0} = \overline{0}$. The zero map is a ring homomorphism, and the only ring homomorphism from $\mathbf{Z}[\sqrt{2}]$ to $\mathbf{Z}_5$.

18. That $\overline{z}_1 + \overline{z}_2 = \overline{z_1+z_2}$ and $\overline{z}_1\,\overline{z}_2 = \overline{z_1 z_2}$ is well known from complex analysis. Complex conjugation is also injective and surjective, and in fact it is its own inverse as $\overline{\overline{z}} = z$.

19. If a and b are in S, then $ab = ba$ as R is commutative. If $ab = 0$ it follows that $a = 0$ or $b = 0$ as R is an integral domain. Finally it is assumed that S has an identity $1_S \neq 0$, so S satisfies the definition of integral domain. [Note that $1_S = 1_R$ necessarily: $1_S\cdot 1_S = 1_S = 1_S\cdot 1_R$, so, by the cancellation property for integral domains, for R, $1_S = 1_R$.]

20. We begin with showing that $\mathbf{Q}[i]$ is a ring by showing it is a subring of $\mathbf{C}$. Clearly $0 = 0+0i$ is in $\mathbf{Q}[i]$. If $\alpha = a+bi$ and $\beta = c+di$ are in $\mathbf{Q}[i]$, then $\alpha-\beta = (a-c)+(b-d)i$ and $\alpha\beta = (ac-bd)+(ad+bc)i$ are in $\mathbf{Q}[i]$ because all of $(a-c)$, $(b-d)$, $(ac-bd)$ and $(ad+bc)$ are in $\mathbf{Q}$. Now that we know $\mathbf{Q}[i]$ is a ring, we note that it contains the identity $1 \neq 0$ of $\mathbf{C}$, so it has an identity $1 \neq 0$, and as $\mathbf{C}$ is commutative, $\mathbf{Q}[i]$ is commutative. The only thing left to check is that every nonzero element has a multiplicative inverse. But in $\mathbf{Q}[i]$, $a+bi = 0$ if and only if $a = b = 0$, so if that is not the case, in $\mathbf{C}$ we can write $(a+bi)^{-1} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$, which is again in $\mathbf{Q}[i]$ if a and b are in $\mathbf{Q}$, not both zero.

21.

(i) To show R is a ring, we show it is a subring of $\mathbf{C}$: $0_{\mathbf{C}} = 0 + 0\cdot\sqrt{2}$ lies in R. Let $\alpha = a+b\sqrt{2}$ and $\beta = c+d\sqrt{2}$ be in R, so a, b, c and $d \in \mathbf{Q}$. Then $\alpha-\beta = (a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2}$ and $\alpha\beta = (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$ lie in R, so that R is a subring of $\mathbf{C}$, hence is a ring. As multiplication in $\mathbf{C}$ is commutative, it is commutative on R as well, so R is commutative. Also $1 = 1+0\cdot\sqrt{2}$ lies in R, and $1\cdot\alpha = \alpha = \alpha\cdot 1$ for all α in R, so that R has an identity, 1. Clearly $1 \neq 0$ in this case. So the only thing that is left to check is that if $\alpha \neq 0$ is in R, then $\alpha\beta = \beta\alpha = 1$ for some β in R. Note that if $\alpha = a+b\sqrt{2} \neq 0$ then $a^2-2b^2 \neq 0$: if $a^2-2b^2 = 0$, either $b = 0$, so then $a = 0$, but then $\alpha = 0$ which is not the case, or $b \neq 0$, and $2 = a^2/b^2 = (a/b)^2$, so that $\sqrt{2}$ would be rational, which is not the case either. Then it is easy to calculate that $\beta = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}$ satisfies $\alpha\beta = \beta\alpha = 1$.

(i) From the definition it is clear that any element in R can be expressed in the form $a+b\sqrt{2}$ with a and b in $\mathbf{Q}$, so we hope $B = \{1, \sqrt{2}\}$ is a basis as it spans R as $\mathbf{Q}$–vector space. Suppose $a+b\sqrt{2} = 0$, with a and b in $\mathbf{Q}$. If $b \neq 0$, then $\sqrt{2} = \frac{-a}{b}$ would be rational, which is not the case. So $b = 0$, and then $a = 0$ as well, showing that 1 and $\sqrt{2}$ are linearly independent over $\mathbf{Q}$. So B is a basis of R as $\mathbf{Q}$–vector space, and $\dim_{\mathbf{Q}}(R) = 2$.

22. (Standard material in textbooks; look for "field of fractions". Specifically, in Peter Cameron's online notes (linked from the course page) look at pp.55–56.)

23. The inverses are $\begin{pmatrix} \overline{1} & \overline{4} & \overline{3} \\ \overline{1} & \overline{0} & \overline{2} \\ \overline{4} & \overline{3} & \overline{3} \end{pmatrix}$ and $\begin{pmatrix} \overline{1} & \overline{2} & \overline{2} \\ \overline{2} & \overline{2} & \overline{0} \\ \overline{2} & \overline{1} & \overline{2} \end{pmatrix}$.

For the first, one set of row operations would be: (1) $R3 := R3+\overline{3}R1$; (2) $R1 := R1+\overline{3}R2$, $R3 := R3+R2$; (3) $R1 := R1-R3$, $R2 := R2-R3$; (4) $R1 := \overline{2}R1$, $R2 := \overline{3}R2$, $R3 := \overline{3}R3$. For the second we could apply (1) $R2 := R2+R1$, $R3 := R3-R1$; (2) $R2 := \overline{2}R2$; (3) $R1 := R1-R2$, $R3 := R3+R1$; (4) $R1 := R1-R3$; (5) $R3 := \overline{2}R3$.

26. The matrix corresponding to this system of equations is the 3×4 matrix with entries in $\mathbf{Z}_7$ given by $\begin{pmatrix} \overline{1} & \overline{3} & \overline{0} & \overline{5} \\ \overline{0} & \overline{3} & \overline{0} & \overline{2} \\ \overline{1} & -\overline{1} & \overline{0} & \overline{0} \end{pmatrix}$. It transforms into $\begin{pmatrix} \overline{1} & \overline{3} & \overline{0} & \overline{5} \\ \overline{0} & \overline{1} & \overline{0} & \overline{3} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} \end{pmatrix}$ under the row operations (1) $R3 := R3-R1$; (2) $R3 := R3-R2$; (3) $R2 := \overline{5}R2$. From this last matrix we can read off a basis of the solution space: $\{(\overline{0},\overline{0},\overline{1},\overline{0}), (\overline{4},\overline{4},\overline{0},\overline{1})\}$. So the solutions of the original linear equations are all linear combinations of the elements in this basis: $\{(\overline{4}\alpha, \overline{4}\alpha, \beta, \alpha)$ with α and β in $\mathbf{Z}_7$ $\}$.

25. Remember that we are assuming the ring has a 1 when talking about units. As $1\cdot 1 = 1$, 1 is in R^*. Then $1\cdot a = a = a\cdot 1$ for all a in R^*. Associativity holds for all elements in R, so in particular in R^*. If a is in R^*, let b in R be such that $ab = ba = 1$ (b exists by the definition of R^*). We have to check that b lies in R^*, i.e., there must exist a c in R with $bc = cb = 1$. Clearly we can take $c = a$. Finally, if a and b are in R^*, with $ac = ca = 1$ and $bd = db = 1$ for some b and d in R, then $(ab)(dc) = a(bd)c = a\cdot 1\cdot c = ac = 1$ and $(dc)(ab) = d(ca)b = d\cdot 1\cdot b = db = 1$, so that ab satisfies the definition to be in R^*. Similarly one checks that ba is in R^* using cd instead of dc.

26. We first show $\varphi(1_R) = 1_S$. Any element s in S is of the form $\varphi(r)$ for some r in R as φ is surjective. So $\varphi(1_R)s = \varphi(1_R)\varphi(r) = \varphi(1_R\cdot r) = \varphi(r) = s$ and similarly $s\varphi(1_R) = s$. This holds for all s in S, so because

S has a unique identity, $\varphi(1_R) = 1_S$. Now let u be in R^*. We must show that $\varphi(u)$ is in S^* rather than S. Let v be in R with $uv = vu = 1_R$. Then $\varphi(u)\varphi(v) = \varphi(v)\varphi(u) = \varphi(1_R) = 1_S$, so $\varphi(u)$ is in S^*. φ is a homomorphism of groups as for any u and v in R^*, $\varphi(uv) = \varphi(u)\varphi(v)$ as φ is a homomorphism of rings. φ is injective, so φ must also be injective on R^*. Finally, to see φ is also surjective, let s be in S^*, so $st = ts = 1_S$ for some t in S^*. As φ is surjective, $s = \varphi(a)$ and $t = \varphi(b)$ for some a and b in R, and we have to see they are in R^*. But $\varphi(ab) = \varphi(a)\varphi(b) = st = 1_S = \varphi(1_R)$, so $ab = 1_R$ as φ is injective. Similarly $ba = 1_R$, so both a and b are in R^*.

27. If $a = ub$ for some u in R^*, let v in R^* be such that $uv = 1$. Then $a = ub$ means $a|b$, but multiplying by v we also get $va = b$, so that $b|a$. (This direction does not use that the ring is an integral domain.) Assume now that $a|b$ and $b|a$, so $b = ca$ and $a = db$ for some c and d in R. Then $1a = a = db = dca$, and the cancellation property for integral domains implies that $a = 0$ or $1 = dc$. If $1 = dc$, d and c must be units because $cd = dc = 1$ as integral domains are commutative. If $a = 0$, then $b = ca = c0 = 0$ as well, so $a = 1b$ and $b = 1a$, and 1 lies in R^*.

28. $\overline{1} + \overline{3}X$ is a unit because $(\overline{1} + \overline{3}X)(\overline{1} + \overline{6}X) = \overline{1} + \overline{9}X + \overline{18}X^2 = \overline{1}$.

29. First of all, if $\alpha|\beta$ in $\mathbf{Z}[i]$, there exists γ in $\mathbf{Z}[i]$ such that $\beta = \gamma\alpha$. As $\beta \neq 0$ in our case, also $\alpha \neq 0$, and we can find γ by computing $\beta\alpha^{-1}$ in $\mathbf{C}$. If $\alpha\gamma = 5$, $N(\alpha)N(\gamma) = N(5) = 25$ (by a previous exercise). Because all norms are in $\mathbf{Z}$ and are nonnegative in this case, we must have $N(\alpha) = 1$, 5 or 25. Note that if $N(\alpha) = N(5) = 25$, then $N(\gamma) = 1$ so that $\gamma = \pm 1$ or $\pm i$. Then $\alpha = \pm 5$ or $\pm 5i$, all of which divide 5 in $\mathbf{Z}[i]$. If $N(\alpha) = 1$, then we have seen that $\alpha = \pm 1$ or $\pm i$, and they divide anything in $\mathbf{Z}[i]$ as they are units. Finally, if $N(\alpha) = 5$, we solve $a^2 + b^2 = 5$ with a and b in $\mathbf{Z}$ in order to find all elements of norm 5 in $\mathbf{Z}[i]$. As then $|a|, |b| \leq 2$, we find the possibilities $\pm(1 \pm 2i)$ and $\pm(2 \pm i)$ (eight elements in total). Then computing $5\alpha^{-1}$ in $\mathbf{C}$ and seeing which of those lie in $\mathbf{Z}[i]$ we see that all those elements divide 5 (note that $5 = (1 + 2i)(1 - 2i) = (2 + i)(2 - i)$). (If we had solved for elements α with $N(\alpha) = 25$, we would also have found candidates $\pm(3 \pm 4i)$ and $\pm(4 \pm 3i)$, which do not divide 5 in $\mathbf{Z}[i]$.)

The cases for 7 and 13 go similarly. For 7, one finds that the elements α dividing 7 must have norm 1, 7 or 49. If $N(\alpha) = 49$, and α divides 7, we find that $\alpha = \pm 7$ or $\pm 7i$, which divide 7. If $N(\alpha) = 1$, we find again the units ± 1 and $\pm i$, also dividing 7. When we try to find elements α with $N(\alpha) = 7$, we have to solve $a^2 + b^2 = 7$ with a and b in $\mathbf{Z}$. If we try the possibilities (clearly $|a|, |b| \leq 2$ here), we find there are no such elements. So all divisors of 7 in $\mathbf{Z}[i]$ are ± 1, $\pm i$, ± 7, $\pm 7i$.

For 13, dealing with $N(\alpha) = 13^2 = 169$ as before yields ± 13 and $\pm 13i$, which divide 13. $N(\alpha) = 1$ leads only to ± 1 and $\pm i$, which divide 13 as well. Finally, solving $N(\alpha) = 13$ gives elements $\pm(2 \pm 3i)$, $\pm(3 \pm 2i)$ (eight elements). All those elements divide 13 (note $13 = (2 + 3i)(2 - 3i) = (3 + 2i)(3 - 2i)$).

For the last part, divide $17 + 41i$ and $3 + 11i$ by $2 + i$ in $\mathbf{C}$ yields $15 + 13i$ and $\frac{17}{5} + \frac{19}{5}i$, so $2 + i$ does divide $17 + 41i$ but it does not divide $3 + 11i$. (Note that $N(2 + i)$ does divide $N(3 + 11i)$ in $\mathbf{Z}$, even though $2 + i$ does not divide $3 + 11i$ in $\mathbf{Z}[i]$.)

30. We use the norm N, $N(a + b\sqrt{-5}) = a^2 + 5b^2$. If α divides 5, $N(\alpha)$ divides $N(5) = 25$, so $N(\alpha) = 1$, 5 or 25. Let $\alpha = a + b\sqrt{-5}$ so $N(\alpha) = a^2 + 5b^2$. It follows that if $N(\alpha) = 1$, then $\alpha = \pm 1$, if $N(\alpha) = 5$, $\alpha = \pm\sqrt{-5}$, and if $N(\alpha) = 25$, $\alpha = \pm 5$, and it is easy to check that all those divide 5.

For 6, this method leads to α with $N(\alpha)$ a positive divisor of $N(6) = 36$, so $N(\alpha) = 1$, 2, 3, 4, 6, 9, 12, 18 or 36. But for those values of d, $a^2 + 5b^2 = d$ has solutions (a, b) in $\mathbf{Z}^2$ only if $d = 1$, 4, 6, 9 or 36, leading to the elements $\alpha = \pm 1$, ± 2, $\pm(1 \pm \sqrt{-5})$, ± 3, $\pm(2 \pm \sqrt{-5})$, $\pm(4 \pm 2\sqrt{-5})$ and ± 6. All those divide 6 (e.g., $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$), except for $\pm(2 \pm \sqrt{-5})$ and $\pm 4 \pm 2\sqrt{-5}$. (Note for this that if $\alpha\beta = 6$, and $N(\alpha) = 36$, $N(\beta) = 1$, so $\beta = \pm 1$, and $\alpha = \pm 6$.)

For 7, this method leads to α with $N(\alpha)$ a positive divisor of $N(7) = 49$, so $N(\alpha) = 1$, 7 or 49. $a^2 + 5b^2 = 7$ does not lead to solutions, so the only divisors are ± 1 and ± 7.

31. If $\alpha|\beta$, then $\beta = \gamma\alpha$ for some γ in $\mathbf{Z}[\sqrt{2}]$. But this then also holds in $\mathbf{Q}[\sqrt{2}]$ (or $\mathbf{C}$), and if $\beta \neq 0$, we can determine γ as $\beta\alpha^{-1}$. Doing this, we find that $17(3 + \sqrt{2})^{-1} = \frac{51}{7} - \frac{17}{7}\sqrt{2}$ does not lie in $\mathbf{Z}[\sqrt{2}]$, so $3 + \sqrt{2}$ does not divide 17 in $\mathbf{Z}[\sqrt{2}]$. For $6 + \sqrt{2}$ we find $(6 + \sqrt{2})(3 + \sqrt{2})^{-1} = \frac{16}{7} + \frac{-3}{7}\sqrt{2}$, so $3 + \sqrt{2}$

does not divide $6+\sqrt{2}$. For $11-8\sqrt{2}$, we get $(11-8\sqrt{2})(3+\sqrt{2})^{-1} = \frac{49}{7} + \frac{-35}{7}\sqrt{2} = 7-5\sqrt{2}$, so that $11-8\sqrt{2} = (7-5\sqrt{2})(3+\sqrt{2})$, and $3+\sqrt{2}$ does divide $11-8\sqrt{2}$ in $\mathbf{Z}[\sqrt{2}]$.

32. Because the degrees of the product of polynomials in $F[X]$ is the sum of the degree of the individual polynomials and the degree of the (constant) polynomial 1 is 0, if $1 = f(X)g(X)$ in $F[X]$, we must have $0 = \deg(1) = \deg(f(X)) + \deg(g(X))$. Clearly $f(X) \neq 0$ and $g(X) \neq 0$, so both $\deg(f(X))$ and $\deg(g(X))$ are nonnegative integers. Then both must be zero, so $f(X)$ and $g(X)$ are elements of F^*. But clearly $F^* \subseteq F[X]^*$, so they must be equal. (If R is an integral domain, the proof that the degrees add up in $F[X]$ works for $R[X]$ as well, and the rest of the argument is the same.)

33. The identity of this ring is $1 = 1 + 0X + 0X^2 + \ldots$ Note that the ring is commutative, so that we only have to find elements u for which there is an element v such that $uv = 1$. If $u = a_0 + a_1X + a_2X^2 + \ldots$ is in $F[[X]]$ with $a_0 = 0$, then for any $v = b_0 + b_1X + b_2X^2 + \ldots$, uv will always have constant term zero, so $a_0 + a_1X + a_2X^2 + \ldots$ cannot be a unit. On the other hand, if $a_0 \neq 0$, by considering the coefficients of the X^i, $uv = 1$ is equivalent to the equations

$$\begin{aligned}
1 &= a_0b_0 \\
0 &= a_0b_1 + a_1b_0 \\
0 &= a_0b_2 + a_1b_1 + a_2b_0 \\
&\vdots \\
0 &= a_0b_k + a_1b_{k-1} + \ldots + a_{k-1}b_1 + a_kb_0 \\
&\vdots
\end{aligned}$$

From the first, we can solve for b_0, then from the second we can solve for b_1, etc., so $v = b_0 + b_1X + b_2X^2 + \ldots$ exists in this case.

34. We use the norm map as in Q.12, so if $\alpha\beta = 1$, then $N(\alpha)N(\beta) = N(1) = 1$ in $\mathbf{Z}$. Because $N(a+b\sqrt{d}) = a^2 - db^2$ and $D < 0$, we can easily solve $a^2 - Db^2 = 1$. If $D = -1$, we have to solve $a^2 + b^2 = 1$, and we find one of a and b must be zero, the other ± 1. This gives the units $\{\pm 1, \pm i\} = \mathbf{Z}[i]^*$. If $D < -1$, $a^2 - Db^2 \geq -Db^2 > 1$ if $b \neq 0$. So $b = 0$, and this gives $a = \pm 1$. Therefore $\mathbf{Z}[\sqrt{D}]^* = \{\pm 1\}$ if $D < -1$.

35.

(i) u is a unit because $u(-1-\sqrt{2}) = 1$ (the ring is commutative, so this is enough). If α is a unit, say $\alpha\beta = 1$, then $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$, and as $N(\alpha)$ and $N(\beta)$ are in $\mathbf{Z}$, it follows $N(\alpha) = N(\beta) = \pm 1$. On the other hand, if $\alpha = a + b\sqrt{2}$ has $N(\alpha) = a^2 - 2b^2 = \pm 1$, then $(a+b\sqrt{2})(a-b\sqrt{2}) = \pm 1$ so $\alpha\left(\pm(a-\sqrt{2})\right) = 1$ and α is a unit.

(ii) If $\pm u^n = \pm u^m$ for some m, n in $\mathbf{Z}$, multiplying by u^{-m} and taking the absolute value we get $|u|^{n-m} = 1$. But $|u| = 0.414\ldots$ so that $n - m = 0$. Then $m = n$ and cancelling $u^m = u^n$ in $\pm u^m = \pm u^n$ we see the signs must match as well.

(iii) We show $(a', b') = (2b - a, a - b)$ is a solution of $X^2 - 2Y^2 = \pm 1$: $(2b-a)^2 - 2(a-b)^2 = 4b^2 - 4ab + a^2 - 2a^2 + 4ab + 2b^2 = 2b^2 - a^2 = \mp 1$. The four inequalities boil down to $2b > a$ and $a > b$. As a and b are at least one, we can verify them by squaring out: $a^2 < 2(a^2 \mp 1) = 4b^2$ if $a > 1$. Also $a^2 = 2b^2 \pm 1 > b^2$ if $b > 1$. Note that $(2b-a)+(a-b)\sqrt{2} = (a+b\sqrt{2})(-1+\sqrt{2}) = (a+b\sqrt{2})(-u)$. If we start with any (a, b) and we iterate this, we get solutions with smaller and smaller a' and b' as long as we have them bigger than one. This must stop when either a or b becomes one, and both are at least one. Then $a = b = 1$ as $a^2 - 2b^2 = \pm 1$. This means that, if we have to do this n times, $(a+b\sqrt{2})(-u)^n = (1+\sqrt{2}) = -u^{-1}$, so $a + b\sqrt{2} = (-1)^{n+1}u^{-n-1}$. Finally we reduce the other cases for a and b to the one we dealt with above. $a = 0$ cannot happen as then $-2b^2 = \pm 1$. If $a > 0$ and $b \leq 0$, $(a, -b)$ is also a solution of $X^2 - 2Y^2 = \pm 1$, so $a - b\sqrt{2} = \pm u^n$ by the above as $a > 0$ and $-b > 0$. Then $a + b\sqrt{2} = \frac{a-b\sqrt{2}}{a-b\sqrt{2}}(a+b\sqrt{2}) = \frac{a^2-2b^2}{a-b\sqrt{2}} = \pm(a-b\sqrt{2})^{-1}$. As we've just seen that $a - b\sqrt{2} = \pm u^n$ for some n, $a + b\sqrt{2} = u^{-n}$ or $-u^{-n}$. So in either of these cases $a + b\sqrt{2} = \pm u^n$

for some n in $\mathbf{Z}$. Finally, if (a,b) is a solution of $X^2-Y^2=\pm 1$ with $a<0$, $(a',b')=(-a,-b)$ is a solution with $a'>0$, which is covered by the previous. This shows that $-(a+b\sqrt{2})=\pm u^n$ for some n in $\mathbf{Z}$, so $a+b\sqrt{2}=\mp u^n$.

36.

(i) $(\overline{1}+\overline{2}X)(\overline{1}+\overline{2}X)=\overline{1}+2\overline{2}X+\overline{2}^2X^2=\overline{1}$, so that $\overline{1}+\overline{2}X$ is a unit, with itself as inverse.

(ii) $(\overline{1}+\overline{2}f(X))(\overline{1}+\overline{2}f(X))=\overline{1}+2\overline{2}f(X)+\overline{2}^2f(X)^2=\overline{1}$, so that $\overline{1}+\overline{2}f(X)$ is a unit, with itself as inverse.

(iii) Because $\mathbf{Z}_2$ is a field, $\mathbf{Z}_2[X]^*=\mathbf{Z}_2^*=\{\overline{1}\}$. The reduction map $\mathbf{Z}_4[X]\to\mathbf{Z}_2[X]$ is a ring homomorphism that maps $1_{\mathbf{Z}_4[X]}$ to $1_{\mathbf{Z}_2[X]}$: they are given by $\overline{1}$ in $\mathbf{Z}_4$ respectively $\mathbf{Z}_2$. So we get an induced map for the respective unit groups $\mathbf{Z}_4[X]^*\to\mathbf{Z}_2[X]^*$ by reduction of the coefficients. This means that if $u(X)$ is a unit in $\mathbf{Z}_4[X]$, it must be equal to $\overline{1}$ after reducing its coefficients modulo 2. Therefore $u(X)-\overline{1}$ must lie in the kernel of the reduction map, and it is easy to check (by looking at coefficients) that this consists of elements of the form $\overline{2}f(X)$. Alternatively, if $u(X)$ becomes $\overline{1}$ after reducing the coefficients modulo 2, the coefficients of X, X^2 etc are either $\overline{0}=\overline{2}\,\overline{0}$, or $\overline{2}=\overline{2}\,\overline{1}$. And the constant term is either $\overline{1}=\overline{1}+\overline{2}\,\overline{0}$, or $\overline{3}=\overline{1}+2\overline{1}$. Putting this together, we get that $u(X)=\overline{1}+\overline{2}f(X)$ for some $f(X)$ in $\mathbf{Z}_4[X]$, as desired.

37. Certainly, if $(X-a)^2$ divides $f(X)$ in $\mathbf{C}[X]$, $f(X)=(X-a)^2g(X)$ for some $g(X)$ and then $f'(X)=2(X-a)g(X)+(X-a)^2g'(X)$. So both $f(a)=0$ and $f'(a)=0$. Conversely, as a is a root of $f(X)$, we can write $f(X)=(X-a)h(X)$ for some $h(X)$ in $\mathbf{C}[X]$. Then $f'(X)=h(X)+(X-a)h'(X)$, and so $0=f'(a)=h(a)$. So again, $h(X)=(X-a)k(X)$ for some $k(X)$ in $\mathbf{C}[X]$, and $f(X)=(X-a)^2k(X)$, i.e., $(X-a)^2$ divides $f(X)$ in $\mathbf{C}[X]$, as desired.

38.

(i) If $|U|=1$ then clearly U is cyclic. If $|U|>1$ write U as in the hint with $k\geq 1$. From Corollary 2.9 in the course, we know that the polynomial $X^{d_k}-1=0$ has at most d_k roots in F. But all elements of U have order dividing d_k because $d_1|d_2|\ldots|d_k$ (check this), so that all elements u of U satisfy $u^{d_k}=1$. This means all $d_1d_2\ldots d_k$ elements of U are roots of $X^{d_k}-1=0$, and as there are at most d_k roots and all $d_i\geq 2$, we must have $k=1$. Then U is isomorphic to $\mathbf{Z}_{d_k}$ so it is cyclic.

(ii) Suppose that -1 is a square in $\mathbf{Z}_p$, say $\alpha^2=-1$. Then $\alpha^4=1$, so that α lies in the group $\mathbf{Z}_p^*$, and the order of α in this equals 1, 2 or 4. If it is 1, we have $\alpha=1$ and $-1=\alpha^2=1$ so that $p=2$. If it is 2, we have $-1=\alpha^2=1$ so that again $p=2$. (As the order is 1 if $p=2$, this case does not really occur.) If the order is 4, we have that 4 divides the order of $\mathbf{Z}_p^*=p-1$ by Lagrange's theorem, so that $p\equiv 1$ modulo 4. For the converse, remember $\mathbf{Z}_p^*$ is a cyclic group of order $p-1$ by the previous part. If $p=2$, then clearly $-1=1=1^2$. If $p\equiv 1$ modulo 4, $p-1=4k$ for some integer k. If α is a generator of $\mathbf{Z}_p^*$, then $\beta=\alpha^{2k}\neq 1$, but $\beta^2=1$. In $\mathbf{Z}_p$ for $p\geq 3$ and prime, there are at most two solutions to $X^2-1=0$, namely ± 1, and they are distinct. so $\beta=-1$.

39. $\overline{0}^p=\overline{0}$. If $\overline{a}\neq\overline{0}$ then $\overline{a}$ is an element in $\mathbf{Z}_p^*$, a group of order $p-1$. Then by Lagrange's theorem, $\overline{a}^{p-1}=\overline{1}$, so $\overline{a}^p=\overline{a}$ as well. Because a polynomial of degree p over a field (like $\mathbf{Z}_p$) has at most p distinct roots, and we have p distinct roots $\overline{0},\overline{1},\ldots,\overline{p-1}$, X^p-X must factorise as $X(X-\overline{1})\ldots(X-\overline{p-1})$ as both are monic.

40. Long division gives us $X^5+4X^4+X+1=(X^3+4X^2-X-4)(X^2+1)+(2X+5)$. Because specialisation yields a homomorphism of rings $\mathbf{Z}[X]\subset\mathbf{Z}[i][X]\to\mathbf{Z}[i]$, and $g(i)=0$, we find $f(i)=5+2i$.

41. We find $X^2+3X+1=(X^2+1)+(3X)$, $X^2+1=(\frac{1}{3}X)(3X)+1$, so that the monic **gcd** equals 1. Then $1=(X^2+1)-(\frac{1}{3}X)(3X)=(X^2+1)-(\frac{1}{3}X)\left((X^2+3X+1)-(X^2+1)\right)=(1+\frac{1}{3}X)(X^2+1)+(-\frac{1}{3}x)(X^2+3X+1)$.

42. This time the polynomials are equal as $\overline{3}=\overline{0}$, so the greatest common divisor is $X^2+\overline{1}$, which is already monic.

43. We find that $f(X) = (X-1)g(X) + 3X^2 + 3$ and $g(X) = (\frac{1}{3}X + \frac{2}{3})(3X^2+3)$. So the (monic) greatest common divisor of $f(X)$ and $g(X)$ is X^2+1, and we can write it as $\frac{1}{3}(3X^2+3) = \frac{1}{3}f(X) - (\frac{1}{3}X - \frac{1}{3})g(X)$.

44. We perform the Euclidean algorithm in each case (the coefficients are in a field).

(i) $X^5 + X^3 + X^2 + 4 = X^2(X^3 + X + 1) + 4$, so the monic gcd is 1.

(ii) Now $X^5 + X^3 + X^2 + \overline{4} = X^2(X^3 + X + \overline{1}) + \overline{0}$, so the monic gcd is $X^3 + X + \overline{1}$.

(iii) $X^4 + 1 = X(X^3+1) + (-X+1)$ and $X^3 + 1 = (-X^2 - X - 1)(-X+1) + 2$, so the monic gcd is 1.

(iv) The calculations are the same as in the previous part, and the monic gcd is $\overline{1}$.

(v) $X^4+3X^2+2 = (X-1)(X^3+X^2+6X+6)+(-2X^2+8)$, $X^3+X^2+6X+6 = (-\frac{1}{2}X-\frac{1}{2})(-2X^2+8)+(10X+10)$, and $(-2X^2+8) = (-\frac{1}{5}X+\frac{1}{5})(10X+10)+6$, so the monic gcd is 1.

(vi) $X^4+3X^2+2 = (X-\overline{1})(X^3+X^2+\overline{6}X+\overline{6})+(\overline{3}X^2+\overline{3})$ and $X^3+X^2+6X+6 = (\overline{2}X+2)(\overline{3}X^2+\overline{3})+\overline{0}$, so the monic gcd is $X^2+\overline{1}$.

(vii) $X^6 - 3X^4 - 2X^2 + 6 = X(X^5 - 3X^3 - X^2 + 3) + (X^3 - 2X^2 - 3X + 6)$; $X^5 - 3X^3 - X^2 + 3 = (X^2+2X+4)(X^3 - 2X^2 - 3X + 6) + (7X^2 - 21)$; $X^3 - 2X^2 - 3X + 6 = (\frac{1}{7}X - \frac{2}{7})(7X^2 - 21) + 0$; So the monic greatest common divisor is $\frac{1}{7}(7X^2 - 21) = X^2 - 3$.

(viii) Here we can take the reduction modulo 3 of the first two steps as in the previous part (or do the calculations again), obtaining $X^6 + X^2 = X(X^5 - X^2) + (X^3 + X^2)$; $X^5 - X^2 = (X^2 + \overline{2}X + \overline{1})(X^3 + X^2) + X^2$; and then $(X^3 + X^2) = (X + \overline{1})X^2 + 0$. So the monic greatest common divisor is X^2.

(ix) Again we can take the reduction of the first two steps of the algorithm over $\mathbf{Q}$ (or do the calculations again), finding: $X^6 - \overline{3}X^4 - \overline{2}X^2 - \overline{1} = X(X^5 - \overline{3}X^3 - X^2 + \overline{3}) + (X^3 - \overline{2}X^2 - \overline{3}X - \overline{1})$; $X^5 - \overline{3}X^3 - X^2 + \overline{3} = (X^2 + \overline{2}X + \overline{4})(X^3 - \overline{2}X^2 - \overline{3}X - \overline{1}) + \overline{0}$. So the monic greatest common divisor is $X^3 - \overline{2}X^2 - \overline{3} - \overline{1}$.

45. q, α and β are in $\mathbf{Z}[i]$, so $r = \alpha - q\beta$ is in $\mathbf{Z}[i]$. For the norm, note that $\alpha/\beta = q + \rho$ means $\alpha = q\beta + \rho\beta$, so that $r = \rho\beta$. Then $N(r) = N(\rho)N(\beta)$, and $N(\rho) = a^2 + b^2 \leq 1/2$, so that in fact $N(r) \leq \frac{1}{2}N(\beta) < N(\beta)$ as $\beta \neq 0$. (N is also multiplicative on $\mathbf{Q}[i]$, see Q.12.)

(i) This is just like for $\mathbf{Z}$:

1. The inequalities for N mean the process must stop as N takes only nonnegative integers as its values, and $N(r_{n+1}) = 0$ only if $r_{n+1} = 0$.

2. The last equation shows that r_n divides r_{n-1}, the second to last equation shows that r_n then also divides the left hand side, i.e. r_{n-2}, etc. Working our way upwards, we find that r_n divides all the left hand sides, and in particular α and $\beta = r_0$. So r_n is a common divisor of α and β.

3. On the other hand, using the first equation, we see that any d which divides α and β also divides r_1, the second equation shows that d then also divides r_2 etc. Working our way downwards, we find that d divides all the r_i and in particular r_n. So combining with 2. shows that r_n is a *greatest* common divisor.

4. In order to express r_n as a linear combination of α and β, start with the second to last equation, $r_n = -q_n r_{n-1} + r_{n-2}$, and substitute successively any r_{n-i}, $i = 1, \ldots, n-1$, using the equation where r_{n-i} stands on the right (i.e., each r_{n-i} is replaced by a linear combination, with coefficients in $\mathbf{Z}[i]$, of r_{n-i-1} and r_{n-i-2}, where we consider α as "r_{-1}"), which results in a linear combination, with coefficients in $\mathbf{Z}[i]$, of α and β.

(ii) Carrying this out, we find $38+41i = (2-i)(8+31i)+(-9-13i)$, $8+31i = (-2-i)(-9-13i)+(3-4i)$, and $-9-13i = (1-3i)(3-4i)$. (Here we used for example that $\frac{38+41i}{8+31i} = \frac{63}{41} - \frac{34}{41}i$, so we can take $q = 2-i$, and then $r = (38+41i) - (2-i)(8+31i)$.) Therefore a gcd is $3-4i$, and it equals $(8+31i) - (-2-i)(-9-13i) = (8+31i) + (2+i)(-9-13i) = (8+31i) + (2+i)((38+41i) - (2-i)(8+31i)) = (2+i)(38+41i) - 4(8+31i)$.

46. α/β equals $a + b\sqrt{2}$ for some a and b in $\mathbf{Q}$. Let c (resp. d) be the integer closest to a (resp. b). Let $q = c + d\sqrt{2}$, which lies in $\mathbf{Z}[\sqrt{2}]$. Then $\alpha/\beta = q + \rho$, with $\rho = (a-c) + (b-d)\sqrt{2}$, and $|a-c|$ and $|b-d|$ at most $\frac{1}{2}$, so that $N'(\rho) = |(a-c)^2 - 2(b-d)^2| \leq (\frac{1}{2})^2 + 2(\frac{1}{2})^2 = \frac{3}{4}$. Put $r = \alpha - q\beta$, so that $\alpha = q\beta + r$. q, α and β are in $\mathbf{Z}[\sqrt{2}]$, so r is in $\mathbf{Z}[\sqrt{2}]$. For the norm, note that $\alpha/\beta = q + \rho$ means $\alpha = q\beta + \rho\beta$, so that $r = \rho\beta$. then $N'(r) = N'(\rho)N'(\beta) \leq \frac{3}{4}N'(\beta) < N'(\beta)$ as $\beta \neq 0$, hence $N'(\beta) \neq 0$. (N and hence N' is also multiplicative on $\mathbf{Q}[\sqrt{2}]$, see Q.12.)

47. We find the roots of X^4+4 by solving $z^4=-4$ in $\mathbf{C}$. Using complex analysis techniques, this leads to the roots $1+i$, $-1+i$, $-1-i$ and $1-i$. So the factorization in $\mathbf{C}[X]$ is $(X-1-i)(X+1-i)(X+1+i)(X-1+i)$. Combining conjugate roots in the above factorization, we find that $X^4+4=(X^2-2X+2)(X^2+2X+2)$ in $\mathbf{R}[X]$. Both factors are irreducible because they have degree two but have no real roots. For the same reason they are irreducible in $\mathbf{Q}[X]$, so that the factorization is the same in $\mathbf{R}[X]$ and $\mathbf{Q}[X]$.

48. By writing out the possible polynomials, and checking the roots, we find that only the polynomials $X^2+X+\overline{1}$, $X^3+X+\overline{1}$ and $X^3+X^2+\overline{1}$ are irreducible of degree 2 or 3.

49. If $f(X)$ is not irreducible, then $f(X)=g(X)h(X)$ with neither $g(X)$ nor $h(X)$ constants. Considering degrees, one of the two factors must have degree one, say $g(X)=aX+b$ with $a\neq 0$. Then $-b/a$ is a root of $g(X)$, and hence of $f(X)$. For the example, take $(X^2+1)^2=X^4+2X^2+1$ in $\mathbf{R}[X]$: it has no roots in $\mathbf{R}$, but is clearly not irreducible.

50. Because of the degree it is sufficient to check that it has no roots, and is not divisible by any of the monic irreducible polynomials of degree 2: $X^2+\overline{1}$, $X^2-X+\overline{2}$ and $X^2+X-\overline{1}$. (They are irreducible because they don't have any roots in $\mathbf{Z}_3$.)

51. $\overline{1}$ is a root, so we can write it as $(X-\overline{1})(X^3+\overline{2}X^2+\overline{3}X+\overline{4})$. The last factor has $\overline{1}$ as a root again, so we can write it as $(X-\overline{1})(X^2+\overline{3}X+\overline{1})$. Again, the last factor has root $\overline{1}$, and it equals $(X-\overline{1})^2$, so that in total we get $(X-\overline{1})^4$.

52. $\overline{2}$ is a root of the first and so is $-\overline{2}=\overline{5}$, so we find $(X-\overline{2})(X+\overline{2})(X^2+\overline{4})$. $X^2+\overline{4}$ has no root, so it is irreducible as it is of degree 2. $X^3-\overline{3}$ is irreducible because it has no roots and is of degree 3.

53. The rational roots for the first polynomial are in $\{\pm 1,\pm 3,\pm 1/2,\pm 3/2\}$. For the second one, they are in $\{\pm 1,\pm 2,\pm 5,\pm 10,\pm 1/7,\pm 2/7,\pm 5/7,\pm 10/7\}$, and for the third, they are in $\{\pm 1,\pm 2,\pm 4\}$. Plugging in, one sees that the first has no roots, the second has only $2/7$ as a root (and factorises as $(X-2/7)(7X^3+35)=(7X-2)(X^3+5)$), and the third one has no roots. (For the last, ± 1 are not roots, and the others cannot be roots because 2^{12} is about 4000, and 4^{12} is about 16×10^6.)

54. For the ones of degree at most three, we can proceed by checking rational roots and using degree arguments. We find $X^2+2X+1=(X+1)^2$, $3X^2+2X+1$ and X^3+X+1 are irreducible. $X^8+164X^6+24X^3+2$ is irreducible by Eisenstein with $p=2$. $X^4+X^3+2X^2+3X+1$ has root -1, and factorises as $(X+1)(X^3+2X+1)$, with the last having no rational root, so it is irreducible for degree reasons. The next factorises as $(2X^2+1)(X^2-X+2)$. This can be found by first noticing that there are no rational roots (same argument as above), so if they factorise it will have to be as two factors of degree two in $\mathbf{Q}[X]$, but by the Gauss lemma, then there is also a factorization into two factors of degree two in $\mathbf{Z}[X]$. Starting with $(aX^2+bX+c)(dX^2+eX+f)$ with $a,\ldots,f$ in $\mathbf{Z}$, we find (among others things) that $ad=2$ for the first one. This means that swapping the two factors and/or multiplying both of them by -1 if necessary, we can assume that $a=2$ and $d=1$, so we get $(2X^2+bX+c)(X^2+eX+f)=2X^4+(b+e)X^3+(2f+be+c)X^2+(bf+ce)X+cf=2X^4-2X^3+5X^2-X+2$. The possibilities for c are ± 1, ± 2, with the corresponding values ± 2, ± 1 for f. The case $c=2$, $f=1$, by equating coefficients, leads to the equations $b+e=-2$, $be=1$ and $b+2e=-1$. $be=1$ is equivalent to $b=e=\pm 1$, but for neither of the two cases do we find a solution. Trying out the possible cases we do find a solution for $c=1$ and $f=2$. The last one is done in a similar way, leading to $(3X^2+X+1)(X^2+X+1)$.

55. For the first one, the possible roots are ± 1, $\frac{\pm 1}{3}$, but none of these are roots. So it is irreducible in $\mathbf{Q}[X]$ by a degree argument. [Note: this is sufficient here only since the degree of the polynomial is ≤ 3.] The second polynomial does not even have real roots, so again it is irreducible by the same degree argument. Since a rational root $b/c\in\mathbf{Q}$ of $f(x)=a_nx^n+\ldots+a_0$ with coprime b, $c\in\mathbf{Z}$ (and non-zero a_n) must satisfy $b|a_0$ and $c|a_n$, the possible roots for the third polynomial are ± 1, ± 5, $\frac{\pm 1}{3}$ and $\frac{\pm 5}{3}$. None of these are roots, so again by the same degree argument, the polynomial is irreducible. The fourth one is an application of Eisenstein's criterion with $p=7$. For the fifth one, we apply the reduction-of-coefficients homomorphism

with $p = 2$, and find the polynomial $X^4 + X^3 + \overline{1}$ (of the same degree) in $\mathbf{Z}_2[X]$. This polynomial has no roots in $\mathbf{Z}_2$, and is not divisible by the (unique) irreducible polynomial of degree 2 in $\mathbf{Z}_2[X]$, $X^2 + X + \overline{1}$ (see Q.48), hence is irreducible, again by the above degree argument.

56. Write $\overline{f}(X)$ for the reduction of $f(X)$ in $\mathbf{Z}_3[X]$. In $\mathbf{Z}_3[X]$, $\overline{f}(X) = X^4 + \overline{2}X^2 + \overline{2}X = X(X^3 + \overline{2}X + \overline{2})$, and the cubic has no root in $\mathbf{Z}_3$, hence is irreducible in $\mathbf{Z}_3[X]$. If $f(X)$ could be factorised in $\mathbf{Q}[X]$, it can be factorised in $\mathbf{Z}[X]$ into terms of the same degree by the Gauss lemma. The possibilities for the degrees (up to swapping the factors) are 1+3 or 1+1+2 or 1+1+1+1 or 2+2. But the last one cannot occur, because reduction modulo 3 would lead to a factorization of $\overline{f}(X)$ involving factors of degree *at most* two (the reductions of the quadratics might have roots in $\mathbf{Z}_3$). So $f(X)$, if it is not irreducible, must have a factor of degree one, and we know that this corresponds to a root of $f(X)$ in $\mathbf{Q}$ by Proposition 2.7. (Arguing as for the solution of Q.55 iii), we find that the only possible roots in $\mathbf{Q}$ are ± 1 and ± 3. None of them are roots, so $f(X)$ is irreducible in $\mathbf{Q}[X]$.)

57. If we reduce the coefficients modulo 2, we get the polynomial $X^4 + X^2 + \overline{1}$ in $\mathbf{Z}_2[X]$, which factorises as $(X^2 + X + \overline{1})^2$. (The quadratic polynomial has no roots in $\mathbf{Z}_2$, so it is irreducible in $\mathbf{Z}_2[X]$.) If we reduce the coefficients modulo 3, we get the polynomial $X^4 + \overline{2}X^2 + \overline{2}X$, which factorises as $X(X^3 + \overline{2}X + \overline{2})$. (The cubic has no roots in $\mathbf{Z}_3$ so it is irreducible in $\mathbf{Z}_3[X]$.) If the original polynomial can be written as a product of two polynomials in in $\mathbf{Q}[X]$, then it would factorise in $\mathbf{Z}[X]$ in two factors of the same degree by the Gauss lemma. So we could write it as $g(X)h(X)$ with $g(X)$ and $h(X)$ in $\mathbf{Z}[X]$, and either $\deg(g(X)) = 1$ and $\deg(h(X)) = 3$ (by swapping the order of the factors if necessary), or $\deg(g(X)) = \deg(h(X)) = 2$. In the first case, the factorization modulo 2 would have to have a factor of degree 1, which is not the case. In the second case the factorization modulo 3 could not have an irreducible factor of degree three, so that cannot happen either. So the polynomial must be irreducible in $\mathbf{Q}[X]$.

58. If $\alpha\beta = 1$, then $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. As $N(a + b\sqrt{-5}) = a^2 + 5b^2$, the only candidates are ± 1, which are clearly units. Similarly, if $\alpha = \beta\gamma$ with β and γ not units, then $N(\alpha) = N(\beta)N(\gamma)$ in $\mathbf{Z}$ with both $N(\gamma), N(\beta) \neq 1$. So for, e.g., $1 + \sqrt{-5}$, with $N(1 + \sqrt{-5}) = 6 = 2 \cdot 3$ we must find elements $a + b\sqrt{-5}$ with $a^2 + 5b^2 = 2$ or 3, but there are none. Similarly one deals with 2 and 3 as $N(2) = 4 = 2 \cdot 2$ and $N(3) = 9 = 3 \cdot 3$. Because ± 2 and ± 3 are not the same as $1 \pm \sqrt{-5}$, the factorizations are distinct.

59.

(i) If $\varphi : R \to \mathbf{R}$ is the indicated map, then $\varphi(f + g) = (f + g)(a) = f(a) + g(a) = \varphi(f) + \varphi(g)$, and $\varphi(fg) = (f \cdot g)(a) = f(a)g(a) = \varphi(f)\varphi(g)$.

(ii) Clearly g lies in $\mathrm{Ker}\,(\varphi)$, so $(g) \subseteq \mathrm{Ker}\,(\varphi)$. If f lies in $\mathrm{Ker}\,(\varphi)$, define h by $h(x) = f(x)/(x - a)$ for $x \neq a$, and by $h(a) = 0$. Then $hg = f$ because $f(a) = 0$, so $f \in (g)$. So in this case indeed $\mathrm{Ker}\,(\varphi) = (g)$. This fails for continuous functions: if again f is in $\mathrm{Ker}\,(\varphi)$, and f were to equal hg for some h, then for any $x \neq a$ we must have $h(x) = f(x)/(x - a)$. But h cannot always be extended to a continuous function on $\mathbf{R}$, e.g., if $f(x) = |x - a|$, so $h(x) = |x - a|/(x - a)$ for $x \neq a$.

60.

(i) We check that I_A is an ideal: the zero function is clearly in I_A. If f and g are in I_A, then for all a in A, $(f - g)(a) = f(a) - g(a) = 0$. And if f is in I_A and g is in R, then $(f \cdot g)(a) = f(a)g(a) = 0$ and $(g \cdot f)(a) = g(a)f(a) = 0$ so $f \cdot g$ and $g \cdot f$ are in I_A. [Of course R is commutative, so $f \cdot g = g \cdot f$.]

(ii) Let $J = \{f$ in R such that $f(x) = 0$ for x large enough$\}$. Then J is an ideal of R: clearly the zero function is in J. If $f(x)$ and $g(x)$ are zero for x large enough, then the same holds for $f(x) - g(x)$, so $f - g$ is in J. And if $f(x)$ is zero for x large enough, and g is in R, then $(f \cdot g)(x) = f(x)g(x)$ is zero for x large enough. As R is commutative, this shows that J is an ideal of R. To show that J is not equal to any I_A, first assume $A \neq \emptyset$, and let a be in A. We can always find a function f_a in J that is nonzero at a (take a function with a "bump"around a, zero everywhere else). Then f_a is in J, but not in I_A so that J and I_A cannot be the same. To show that $J \neq I_\emptyset$, note that $I_\emptyset = R$ as there is no condition in this case. But not all functions in R are zero for x large enough, so we cannot have $J = I_\emptyset$ either.

61. If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is in $M_2(\mathbf{R})$, then I will also have to contain $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ c & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} A & B \\ 0 & 0 \end{smallmatrix}\right)$ for all a, b, c, d, A, B, C and D in $\mathbf{R}$. In particular I must contain $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, so it must contain $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & A \\ 0 & C \end{smallmatrix}\right)$, for all A, B, C and D in $\mathbf{R}$. So for any a, b, c and d in $\mathbf{R}$, putting $A = b$ and $C = d$, I must contain $\left(\begin{smallmatrix} a & 0 \\ c & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & b \\ 0 & d \end{smallmatrix}\right)$, hence their sum $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

62.

(i) Let $K = \varphi^{-1}(J)$. We check that K is an ideal of R: 0_R is in K because $\varphi(0_R) = 0_S$, and 0_S is in J because it is an ideal of S. If k_1 and k_2 are in K, so $\varphi(k_1)$ and $\varphi(k_2)$ are in J, then $k_1 - k_2$ is in K because $\varphi(k_1 - k_2) = \varphi(k_1) - \varphi(k_2)$ is in J as J is a subgroup of S under addition. If k is in K and r is in R, then $\varphi(rk) = \varphi(r)\varphi(k)$ is in J because $\varphi(k)$ is in J and J is an ideal of S. Similarly kr is in K.

(i) In general the image of an ideal is not an ideal. For example, take $R = \mathbf{Z}$ and $S = \mathbf{Q}$, with the inclusion map (a ring homomorphism because $\mathbf{Z}$ is a subring of $\mathbf{Q}$). Then $\mathbf{Z}$ is an ideal of $\mathbf{Z}$, but $\mathbf{Z}$ is not an ideal of $\mathbf{Q}$, as $\mathbf{Q}$ is a field so it has only the ideals $\{0\}$ and $\mathbf{Q}$. If $\varphi : R \to S$ is surjective, and I is an ideal of R, then $\varphi(I)$ is an ideal of S: φ is a homomorphism of groups with respect to addition. That doesn't use the surjectivity, but the last bit does: if j is in $\varphi(I)$, and s is in S, then there exist i in I with $\varphi(i) = j$ by definition of $\varphi(I)$ and r in R with $\varphi(r) = s$ because φ is surjective. Then $sj = \varphi(r)\varphi(i) = \varphi(ri)$ is in $\varphi(I)$ as ri is in I: I is an ideal of R. Similarly js is in $\varphi(I)$.

63. Certainly, if $(A) \subseteq I$, then $a = 1 \cdot a$ lies in $(A) \subseteq I$ for all $a \in A$. On the other hand, assume that $a \in I$ for all $a \in A$. An element in (A) is of the form $\sum_a r_a a$ for some r_a in R (and the sum is finite). Each $r_a a$ lies in I as a lies in $A \subseteq I$ and I is Because ideals are additive subgroups $\sum_a r_a a$ lies in I as well, so we get $(A) \subseteq I$.

64. Showing that φ is a ring homomorphism is straightforward using that $\overline{5}^2 = \overline{25} = \overline{-1}$ in $\mathbf{Z}_{13}$. To show the kernel is of the required shape, note that if $a+bi$ is in $\mathrm{Ker}\,(\varphi)$, then $a+bi = a+5b+b(-5+i) = 13k+b(-5+i)$ for some k in $\mathbf{Z}$, so $a + bi$ lies in $(-5 + i, 13)$. Conversely, it is easy to check that 13 and $-5 + i$ are in the kernel, so any element of the form $\alpha 13 + \beta(-5 + i)$ will go to $\overline{0}$ as φ is a ring homomorphism. That shows that $(-5 + i, 13) \subseteq \mathrm{Ker}\,(\varphi)$ as well, so $(-5 + i, 13) = \mathrm{Ker}\,(\varphi)$. To see that $(-5 + i, 13) = (3 + 2i)$, we verify that $3 + 2i$ is in $\mathrm{Ker}\,(\varphi)$, so $(3 + 2i) \subseteq \mathrm{Ker}\,(\varphi) = (-5 + i, 13)$. We also note that $13 = (3 - 2i)(3 + 2i)$ and $-5 + i = (-1 + i)(3 + 2i)$ are in $(3 + 2i)$, so that $(-5 + i, 13) \subseteq (3 + 2i)$ as well by Q.63.

65. That φ is a homomorphism of rings is straightforward using that $\overline{7}^2 = -\overline{1}$ in $\mathbf{Z}_{25}$. It is surjective because $\mathbf{Z}_{25} = \{\overline{0}, \overline{1}, \ldots, \overline{24}\}$ and $0, 1, \ldots, 24$ map to those elements under φ. In order to find the kernel, we see that any element in the kernel is of the form $a + bi = a + 7b + b(-7 + i) = 25k + b(-7 + i)$ for some k in $\mathbf{Z}$, so that $\mathrm{Ker}\,(\varphi) \subseteq (25, -7 + i)$. Note that 25 and $-7 + i$ are in the kernel of φ, so any element of the form $\alpha 25 + \beta(-7 + i)$ lies in $\mathrm{Ker}\,(\varphi)$: $\varphi(\alpha 25 + \beta(-7 + i)) = \varphi(\alpha)\varphi(25) + \varphi(\beta)\varphi(-7 + i) = \overline{0}$. So $\mathrm{Ker}\,(\varphi) = (25, -7 + i)$. If $(25, -7 + i) = (\gamma)$ for some γ in $\mathbf{Z}[i]$, we must have that γ divides both 25 and $-7 + i$ in $\mathbf{Z}[i]$. Because $N(25) = 25^2$ and $N(-7 + i) = 7^2 + 1^2 = 50$, it could only be an element c with $N(\gamma)$ dividing those numbers, so that $N(\gamma) = 1$, 5 or 25. Trying gives that $3 - 4i$ divides both $25 = (3 - 4i)(3 + 4i)$ and $-7 + i = (3 - 4i)(-1 - i)$. Then any element of the form $\alpha 25 + \beta(-7 + i) = [\alpha(3 + 4i) + \beta(-1 - i)](3 - 4i)$ is in $(3 - 4i)$, so that $\mathrm{Ker}\,(\varphi) = (25, -7 + i) \subseteq (3 - 4i)$. On the other hand, any element of the form $\delta(3 - 4i)$ is in the kernel, as $\varphi(\delta(3 - 4i)) = \varphi(\delta)\varphi(3 - 4i) = \varphi(\delta)\overline{0} = \overline{0}$. Therefore $\mathrm{Ker}\,(\varphi) = (3 - 4i)$.

66. If I is in R, then 1_R is in both I and R^* (the units of R). If I contains some element u in R^*, let v in R be such that $vu = 1$. Then $r = r \cdot 1 = (rv)u$ lies in I for all r in R, so $R \subseteq I$, and they must be equal (as $I \subseteq R$ by definition).

67. If the ideal were of the form (a), a would divide both 3 and $1 + \sqrt{-5}$, so $N(a)$ would divide $N(3) = 9$ and $N(1 + \sqrt{-5}) = 6$, so $N(a)$ would equal 1 or 3. There are no elements with norm three, and the only elements with norm 1 are ± 1, in which case the ideal would equal R. If this were the case, we could write

$1 = (a + b\sqrt{-5})3 + (c + d\sqrt{-5})(1 + \sqrt{-5}) = (3a + c - 5d) + (3b + c + d)\sqrt{-5}$ for some a, b, c and d in $\mathbf{Z}$. This means that $3a + c - 5d = 1$ and $3b + c + d = 0$. The last tells us that $\overline{c + d} = \overline{0}$ in $\mathbf{Z}_3$, but the first says that $\overline{c + d} = \overline{1}$ in $\mathbf{Z}_3$, so that is impossible. Hence the ideal is not principal.

68. Write $d = xa + yb$ for some x and y in $\mathbf{Z}$, so for any integer k, $kd = kxa + kyb$ is in (a, b), and hence $(d) \subseteq (a, b)$. Conversely, if $a = md$ and $b = nd$, then the elements in (a, b) are of the form $sa + tb = smd + tnd = (sm + tn)d$ for s and t in $\mathbf{Z}$, so $(a, b) \subseteq (d)$ as well. [We could also refer to Q.63, noticing that a and b are multiples of d, so they lie in (d), and that $d = xa + by$ for some integers x and y, so d lies in (a, b).]

69. Clearly, $\{0\} = (0)$ is principal, so assume $I \neq \{0\}$. Let $\alpha \neq 0$, $\alpha \in I$, have lowest norm among the nonzero elements of I. (Such α exists because the norms of the nonzero elements in I form a subset of $\mathbf{N}$.) According to Q.45, if β lies in I, we can write $\beta = q\alpha + r$ with q and r in $\mathbf{Z}[i]$, and $N(r) < N(\alpha)$. Because $r = \beta - q\alpha$, r is in I. Because α has lowest norm among the *nonzero* elements of i, we must have $r = 0$. This shows that $I \subseteq (\alpha)$. But as α lies in I, we also have $(\alpha) = \mathbf{Z}[i]\alpha \subseteq I$ so that $(\alpha) = I$.

70. Suppose that $(X, 2) = (f(X))$ for some $f(X)$ in $\mathbf{Z}[X]$. Then $2 = g(X)f(X)$ for some $g(X)$ in $\mathbf{Z}[X]$, so (working in $\mathbf{Q}[X]$), we see that $f(X)$ and $g(X)$ must have degree 0, and are elements of $\mathbf{Z}$. Then $f(X) = \pm 1$ or ± 2. If $f(X) = \pm 2$, because X lies in $(X, 2) = (f(X))$, $X = h(X)(\pm 2)$ for some $h(X)$ in $\mathbf{Z}[X]$, which cannot happen because the coefficients in $h(X)(\pm 2)$ are even. So $f(X) = \pm 1$. Then 1 lies in $(f(X)) = (X, 2)$, so $1 = a(X)X + b(X)2$ for some $a(X)$ and $b(X)$ in $\mathbf{Z}[X]$. Substituting 0 for X (this is nothing but to apply the specialisation homomorphism $\mathbf{Z}[X] \to \mathbf{Z}$), we find that $1 = a(0)0 + b(0)2 = b(0)2$ in $\mathbf{Z}$, which is impossible. This gives a contradiction, from which we can conclude that $(X, 2)$ cannot be a principal ideal in $\mathbf{Z}[X]$.

71.

(i) If $\alpha = a + bi$ is in R, then we can write $a = 2k + a'$ and $b = 2l + b'$ with k and l in $\mathbf{Z}$, and $a' = 0$ or 1, $b' = 0$ or 1. Then $\alpha = (a' + b'i) + (k + li)2$, so $\overline{\alpha} = \overline{a' + b'i}$, showing that there are at most the four given elements in R/I. In order to check that they are all different, assume $\overline{a' + b'i} = \overline{c' + d'i}$ with a', b', c' and d' in $\{0, 1\}$. Then $\overline{(a' - c') + (b' - d')i} = \overline{0}$, so $(a' - c') + (b' - d')i$ is in I, i.e., $(a' - c') + (b' - d')i = (e + fi)2 = 2e + 2fi$ for some e and f in $\mathbf{Z}$. But $a' - c' = 0$ or ± 1, so we must have $a' = c'$. Similarly $b' = d'$, and therefore all four given elements in R/I are different.

(ii)

$+$	$\overline{0}$	$\overline{1}$	$\overline{i}$	$\overline{1+i}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{i}$	$\overline{1+i}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1+i}$	$\overline{i}$
$\overline{i}$	$\overline{i}$	$\overline{1+i}$	$\overline{0}$	$\overline{1}$
$\overline{1+i}$	$\overline{1+i}$	$\overline{i}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{i}$	$\overline{1+i}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{i}$	$\overline{1+i}$
$\overline{i}$	$\overline{0}$	$\overline{i}$	$\overline{1}$	$\overline{1+i}$
$\overline{1+i}$	$\overline{0}$	$\overline{1+i}$	$\overline{1+i}$	$\overline{0}$

(Note that both addition and multiplication are commutative in this ring, so we do not have to indicate how to read the tables.)

In the tables, we sometimes have to identify which of the four elements we get. E.g., $\overline{i} \cdot \overline{i} = \overline{i^2} = \overline{-1} = \overline{1}$ as $1 - (-1) = 2$ is in I.

R/I is not a field: $\overline{1+i} \neq 0_{R/I} = \overline{0}$, but from the multiplication table we see that there is no element a in R/I such that $a \cdot \overline{1+i} = 1_{R/I} = \overline{1}$. Alternatively, $\overline{1+i} \neq 0_{R/I}$, but $(\overline{1+i})^2 = \overline{0} = 0_{R/I}$, so that R/I is not even an integral domain.

(iii) Note that the diagonal of the addition table for R/I tells us that every element in R/I has order 1 or 2. As $\mathbf{Z}_4$ has two elements of order 4, this means that R/I and $\mathbf{Z}_4$ are not even isomorphic as groups under addition, hence certainly not as rings. This argument does not work for $\mathbf{Z}_2 \times \mathbf{Z}_2$. (In fact, R/I and $\mathbf{Z}_2 \times \mathbf{Z}_2$ are isomorphic as groups under addition.) But every element x in $\mathbf{Z}_2 \times \mathbf{Z}_2$ satisfies $x^2 = x$. This property would be preserved under a ring isomorphism, but in R/I this fails for $\overline{i}$ and $\overline{1+i}$. So R/I and $\mathbf{Z}_2 \times \mathbf{Z}_2$ cannot be isomorphic as rings.

72. We have to remember that, if I is an ideal in a ring R, then in R/I, $\overline{a}\,\overline{b} = \overline{ab}$, and $\overline{c} = \overline{d}$ if and only if $c - d$ lies in I. Here we have to check if $(3 + 2i)(4 + 3i) - (-7 + 6i) = 13 + 11i$ lies in $(5 + 2i)$ in $\mathbf{Z}[i]$. As $\frac{13+11i}{5+2i} = 3 + i$ this is the case, so the answer is yes.

73. As in a general quotient ring R/I, $\overline{\alpha}\,\overline{\beta} = \overline{\gamma}$ if and only if (in R) $\alpha\beta - \gamma$ lies in I, we have to check if any of $(2+i)(1+i)-2$, $(2+i)(1+i)-(1-i)$ and $(2+i)(1+i)-(-1-i)$ lie in $(3+i) = \{\alpha(3+i)$ with α in $\mathbf{Z}[i]\}$. We can do this by simply dividing each of those expressions by $3+i$ and see if the quotient is in $\mathbf{Z}[i]$. We find this is the case for the first and the last, but not the middle. So $\overline{2+i} \cdot \overline{1+i} = \overline{2} = \overline{-1-i}$ but it is not equal to $\overline{1-i}$.

74. Let $\varphi : R \to S$ be a homomorphism of rings, I an ideal of R, and $\pi : R \to R/I$ the canonical projection. Show that if there exists a ring homomorphism $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi} \circ \pi = \varphi$, then $I \subseteq \mathrm{Ker}\,(\varphi)$. [This shows that the condition $I \subseteq \mathrm{Ker}\,(\varphi)$ in Proposition 3.14 is necessary.]

75.

(i) $\varphi((a_1+b_1i)+(a_2+b_2i)) = \varphi((a_1+a_2)+(b_1+b_2)i) = \overline{a_1+a_2+4b_1+4b_2}$. This equals $\varphi(a_1+b_1i)+\varphi(a_2+b_2i) = \overline{a_1+4b_1+a_2+4b_2}$. $\varphi((a_1+b_1i)(a_2+b_2i)) = \varphi((a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i) = \overline{a_1a_2-b_1b_2+4(a_1b_2+a_2b_1)}$. On the other hand, $\varphi(a_1+b_1i)\varphi(a_2+b_2i) = \overline{(a_1+4b_1)} \cdot \overline{(a_2+4b_2)} = \overline{a_1a_2+4(a_1b_2+a_2b_1)+16b_1b_2}$. The two are equal as $\overline{16} = \overline{-1}$ in $\mathbf{Z}_{17}$. The homomorphism is surjective because $0, 1, \ldots, 16$ map to all the elements $\overline{0}, \overline{1}, \ldots, \overline{16}$ in $\mathbf{Z}_{17}$.

(ii) Elements in $(-4+i)$ are of the form $(a+bi)(-4+i)$, and then $\varphi((a+bi)(-4+i)) = \varphi(a+bi)\varphi(-4+i) = \varphi(a+bi)\overline{0} = \overline{0}$.

(iii) Let $a+bi$ lie in the kernel of φ. Writing $a+bi = a+4b+b(-4+i)$, so $\varphi(a+bi) = \overline{a+4b} = \overline{0}$ means that 17 divides $a+4b$ in $\mathbf{Z}$, say $a+4b = k17$. As $17 = (-4-i)(-4+i)$ in $\mathbf{Z}[i]$, $a+bi = k(-4-i)(-4+i)+b(-4+i) = (-4k+b-ki)(-4+i)$ lies in $(-4+i)$ as desired.

(iv) We can apply the first isomorphism theorem: we know φ is a surjective ring homomorphism with kernel $(-4+i)$, so $\mathbf{Z}[i]/(-4+i) \cong \mathbf{Z}_{17}$.

76.

(i) If $\alpha = a+b\sqrt{5}$ and $\beta = c+d\sqrt{5}$ are in R, then $\varphi(\alpha+\beta) = \varphi((a+c)+(b+d)\sqrt{5}) = \overline{(a+c)+(b+d)} = \overline{a+b+c+d}$ and $\varphi(\alpha)+\varphi(\beta) = \overline{a+b}+\overline{c+d} = \overline{a+b+c+d}$ as well. Also, $\varphi(\alpha \cdot \beta) = \varphi((ac+5bd)+(ad+bc)\sqrt{5}) = \overline{(ac+5bd)+(ad+bc)} = \overline{ac+ad+bc+bd}$ as $\overline{5} = \overline{1}$ in $\mathbf{Z}_2$. On the other hand, $\varphi(\alpha) \cdot \varphi(\beta) = \overline{a+b} \cdot \overline{c+d} = \overline{(a+b)(c+d)} = \overline{ac+ad+bc+bd}$ as well, so φ is a homomorphism of rings. Note that $\varphi(2) = \overline{2+0} = \overline{0}$ and $\varphi(1+\sqrt{5}) = \overline{1+1} = \overline{0}$ so that both 2 and $1+\sqrt{5}$ lie in $\mathrm{Ker}\,(\varphi)$. By Q.63 we get that $(2, 1+\sqrt{5}) \subseteq \mathrm{Ker}\,(\varphi)$ because $\mathrm{Ker}\,(\varphi)$ is an ideal of R.

(ii) We now only have to show that $\mathrm{Ker}\,(\varphi) \subseteq (2, 1+\sqrt{5})$ as we know the reverse inclusion from (i). If $\alpha = a+b\sqrt{5}$ is in $\mathrm{Ker}\,(\varphi)$, then $\overline{a+b} = \overline{0}$, so that $a+b = 2k$ for some k in $\mathbf{Z}$. Then $\alpha = a+b\sqrt{5} = a-b+b(1+\sqrt{5}) = (k-b)2+b(1+\sqrt{5})$ lies in $(2, 1+\sqrt{5})$.

(iii) We of course apply the first isomorphism theorem (for rings), but before doing so we still have to check that φ is surjective. Clearly, $\varphi(0) = \overline{0}$ and $\varphi(1) = \overline{1}$ so φ is surjective. As we now know that φ is a surjective ring homomorphism with $\mathrm{Ker}\,(\varphi) = (2, 1+\sqrt{5})$, we get that $R/(2, 1+\sqrt{5}) \cong \mathbf{Z}_2$.

77.

(i) If $\alpha = a+b\sqrt{5}$ and $\beta = c+d\sqrt{5}$ are in R, then $\varphi(\alpha+\beta) = \varphi((a+c)+(b+d)\sqrt{5}) = \overline{(a+c)+(b+d)} = \overline{a+b+c+d}$ and $\varphi(\alpha)+\varphi(\beta) = \overline{a+b}+\overline{c+d} = \overline{a+b+c+d}$ so they agree. Also, $\varphi(\alpha \cdot \beta) = \varphi((ac+7bd)+(ad+bc)\sqrt{5}) = \overline{(ac+7bd)+4(ad+bc)} = \overline{ac+4ad+4bc+7bd}$, and $\varphi(\alpha)\varphi(\beta) = \overline{a+4b} \cdot \overline{c+4d} = \overline{ac+4ad+4bc+16bd}$ and the two agree as $\overline{16} = \overline{7}$ in $\mathbf{Z}_9$. Note that $\varphi(9) = \overline{9+0} = \overline{0}$ and $\varphi(4-\sqrt{5}) = \overline{4+4 \cdot (-1)} = \overline{0}$ so that both 9 and $4-\sqrt{5}$ lie in the ideal $\mathrm{Ker}\,(\varphi)$. By Q.63 we get that $(9, 4-\sqrt{5}) \subseteq \mathrm{Ker}\,(\varphi)$ as $\mathrm{Ker}\,(\varphi)$ is an ideal of R.

(ii) We now only have to show that $\mathrm{Ker}\,(\varphi) \subseteq (9, 4-\sqrt{5})$ as we know the reverse inclusion from (i). If $\alpha = a+b\sqrt{5}$ is in $\mathrm{Ker}\,(\varphi)$, then $\overline{a+4b} = \overline{0}$, so that $a+4b = 9k$ for some k in $\mathbf{Z}$. Then $\alpha = a+b\sqrt{5} = a+4b-b(4-\sqrt{5}) = 9k-b(4-\sqrt{5})$ lies in $(9, 4-\sqrt{5})$.

(iii) We apply the first isomorphism theorem, but before doing so we still have to check that φ is surjective. Clearly, φ maps $0, 1, \ldots, 8$ to $\overline{0}, \overline{1}, \ldots, \overline{8}$ so φ is surjective. Then φ is a surjective ring homomorphism with $\mathrm{Ker}\,(\varphi) = (9, 4-\sqrt{5})$, so we get that $R/(9, 4-\sqrt{5}) \cong \mathbf{Z}_9$.

78. Define a map $\varphi : \mathbf{Z}_3[X] \to \mathbf{Z}_3$ by mapping $f(X)$ to $f(2)$, so that $X+1$ is in the kernel. This is a ring homomorphism (as it is a specialisation homomorphism). If $f(X)$ is in $(X+1)$, $f(X) = g(X)(X+1)$ for some

$g(X)$ in $\mathbf{Z}_3[X]$, and $\varphi(f(X)) = \varphi(g(X))\varphi(X+1) = 0$. If $f(X)$ lies in $\mathrm{Ker}\,(\varphi)$, write $f(X) = q(X)(X+1)+c$ for some $q(X)$ in $\mathbf{Z}_3[X]$ and c a polynomial of degree at most 0, i.e., an element of $\mathbf{Z}_3$. Then $\varphi(f(X)) = c$, so $c = 0$, and $f(X)$ is in $(X+1)$. This shows that $\mathrm{Ker}\,(\varphi) = (X+1)$. φ is surjective because it maps 0, 1 and 2 in $\mathbf{Z}_3[X]$ to 0, 1 and 2 in $\mathbf{Z}_3$. So by the first isomorphism theorem we get an isomorphism $\mathbf{Z}_3[X]/(X+1) \cong \mathbf{Z}_3$.

79.

(i) $\varphi(X^2-2) = \sqrt{2}^2 - 2 = 0$, so if $f(X)$ lies in the ideal (X^2-2), $f(X) = g(X)(X^2-2)$ for some $g(X)$ in $\mathbf{Q}[X]$, and $\varphi(f(X)) = \varphi(g(X))\varphi(X^2-2) = \varphi(g(X))0 = 0$. This shows that $(X^2-2) \subseteq \mathrm{Ker}\,(\varphi)$. If $h(X)$ is in $\mathrm{Ker}\,(\varphi)$, write $h(X) = (X^2-2)q(X) + (a+bX)$ with a and b in $\mathbf{Q}$ (use division with remainder). Then $0 = \varphi(h(X)) = \varphi(a+bX) = a + b\sqrt{2}$. $\sqrt{2}$ is irrational, so $a = b = 0$. Hence $h(X)$ is in (X^2-2), and $\mathrm{Ker}\,(\varphi) \subseteq (X^2-2)$ as well.

(ii) If $f(X)$ is in $\mathbf{Q}[X]$, then we can still write $f(X) = q(X)(X^2-2) + (a+bX)$ with a and b in $\mathbf{Q}$. Then $\varphi(f(X)) = a + b\sqrt{2}$ lies in $\mathbf{Q}[\sqrt{2}]$. φ is surjective onto $\mathbf{Q}[\sqrt{2}]$ as $a+bX$ maps to $a+b\sqrt{2}$ for a and b in $\mathbf{Q}$. Because φ is a surjective ring homomorphism with kernel (X^2-2) and image $\mathbf{Q}[\sqrt{2}]$, the first isomorphism theorem gives us an isomorphism of rings $\mathbf{Q}[X]/(X^2-2) \cong \mathbf{Q}[\sqrt{2}]$.

80.

(i) Note that for a in $\mathbf{Z}$, $A = \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ lies in R and $\varphi(A) = a$, so φ is surjective. Let $\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right)$ be in R. Then $\varphi(\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right)) = \varphi(\left(\begin{smallmatrix} a_1+a_2 & b_1+b_2 \\ 0 & c_1+c_2 \end{smallmatrix}\right)) = a_1 + a_2 = \varphi(\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right)) + \varphi(\left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right))$ and $\varphi(\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right)) = \varphi(\left(\begin{smallmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{smallmatrix}\right)) = a_1a_2 = \varphi(\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right))\varphi(\left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right))$ so that φ is a homomorphism of rings.

(ii) $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ is in $\mathrm{Ker}\,(\varphi)$ if and only if $a = 0$, so that $\mathrm{Ker}\,(\varphi) = \{\left(\begin{smallmatrix} 0 & b \\ 0 & c \end{smallmatrix}\right)$ with b and c in $\mathbf{Z}\}$. By the first isomorphism theorem we now get that $R/\mathrm{Ker}\,(\varphi) \cong \mathbf{Z}$ as φ is a surjective homomorphism of rings. The elements in $R/\mathrm{Ker}\,(\varphi)$ are the cosets *with respect to addition* of $\mathrm{Ker}\,(\varphi)$, so the elements of $R/\mathrm{Ker}\,(\varphi)$ are of the form $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) + \mathrm{Ker}\,(\varphi) = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) + \{\left(\begin{smallmatrix} 0 & d \\ 0 & e \end{smallmatrix}\right)$ with d and e in $\mathbf{Z}\} = \{\left(\begin{smallmatrix} a & B \\ 0 & C \end{smallmatrix}\right)$ with B and C in $\mathbf{Z}\}$. $R/\mathrm{Ker}\,(\varphi) \cong \mathbf{Z}$ is given by picking out the upper left entry a: $\overline{\varphi}(\overline{x}) = \varphi(x)$ in the first isomorphism theorem here means that if $\overline{x} = \{\left(\begin{smallmatrix} a & B \\ 0 & C \end{smallmatrix}\right)$ with B and C in $\mathbf{Z}\}$, pick any element x in $\overline{x}$, so $x = \left(\begin{smallmatrix} a & B \\ 0 & C \end{smallmatrix}\right)$ for some B and C in $\mathbf{Z}$. Then we compute $\varphi(x)$, which gives us a. This is independent of the choice of x in $\overline{x}$, i.e., the choice of B and C in $\mathbf{Z}$.

81. First we show that $I \cdot J + I \cdot K \subseteq I \cdot (J+K)$. Note that $I \cdot (J+K)$ is an ideal, so in particular is closed under addition. So $I \cdot J + I \cdot K$ is contained in it if we can show that $I \cdot J$ and $I \cdot K$ are contained in it. But $J \subseteq J+K$, so $I \cdot J \subseteq I \cdot (J+K)$, and $K \subseteq J+K$ so $I \cdot K \subseteq I \cdot (J+K)$ as well. Next we show that $I \cdot (J+K) \subseteq I \cdot J + I \cdot K$. An element in $J+K$ is of the form $j+k$ with j in J and k in K. An element in $I \cdot (J+K)$ is then of the form: a finite sum of elements $i(j+k)$ with i in I, j in J and k in K. As $i(j+k) = ij + ik$, we can rewrite such an element as a finite sum of terms of the form ij, plus a finite sum of terms of the form ik. But the finite sum of ij's is in $I \cdot J$, and the finite sum of ik's is in $I \cdot K$, so that the element is in $I \cdot J + I \cdot K$.

82. Let $I = (a_1, \ldots, a_m)$ and $J = (b_1, \ldots, b_n)$, $K = (a_1, \ldots, a_m, b_1, \ldots, b_n)$ so we have to check if $I + J = K$. Clearly $a_i = a_i + 0$ is in $I + J$ and similarly for the b_j so by Q.63 $K \subseteq I + J$. On the other hand, by Q.63 again, $I \subseteq K$ and $J \subseteq K$. As K is an ideal (so it is closed under addition), if i is in $I \subseteq K$ and j is in $J \subseteq K$, then $i+j$ is in K. This shows that $I + J \subseteq K$ as well. Now let $L = (a_1 \cdot b_1, \ldots, a_1 \cdot b_n, \ldots, a_m \cdot b_1, \ldots, a_m \cdot b_n)$. Then $a_i \cdot b_j$ is in $I \cdot J$ by the definitions, so by Q.63, $L \subseteq I \cdot J$. On the other hand, an element in $I \cdot J$ looks like a finite sum of terms that look like $(\sum_{k=1}^m r_k a_k)(\sum_{l=1}^n r_l b_l)$ for r_k and r_l in R. As L is an ideal (so it is closed under addition), we only have to check that each of those terms is of the form $\sum_{i=1}^m \sum_{j=1}^n r_{i,j} a_i b_j$ with all $r_{i,j}$ in R. But R is commutative, so $(\sum_{k=1}^m r_k a_k)(\sum_{l=1}^n r_l b_l) = \sum_{k=1}^m \sum_{l=1}^n r_k r_l a_k b_l$ so that is the case. This shows that $I \cdot J \subseteq L$ as well. [Note that we used that R has an identity to see that a_j is in $(a_1, \ldots, a_m) = \{\sum_{k=1}^m r_k a_k$ with all r_k in $R\}$ and similarly for b_j. The commutativity of R is also used to see that $\{\sum_{k=1}^m r_k a_k$ with all r_k in $R\}$ is indeed an ideal.]

83. $\mathbf{Z}[\sqrt{5}]$ is a commutative ring with identity, so we use Q.63 to check if two ideals are equal by working at the level of generators.

(i) We always have $(2, 3\sqrt{5}) \subseteq (1)$ as $(1) = \mathbf{Z}[\sqrt{5}]$. For the reverse inclusion, notice that $1 = (-7) \cdot 2 + \sqrt{5} \cdot 3\sqrt{5}$ is in $(2, 3\sqrt{5})$.

(ii) $(1 + \sqrt{5}) \subseteq (7 + 3\sqrt{5}, 1 + \sqrt{5})$ clearly as $1 + \sqrt{5} = 0 \cdot (7 + 3\sqrt{5}) + 1 \cdot (1 + \sqrt{5})$. For the reverse inclusion notice that $-4 = (1 - \sqrt{5})(1 + \sqrt{5})$ is in $(1 + \sqrt{5})$, so $7 + 3\sqrt{5} = (-1) \cdot (-4) + 3 \cdot (1 + \sqrt{5})$ is in $(1 + \sqrt{5})$. [You could find this by computing $(7 + 3\sqrt{5})/(1 + \sqrt{5}) = 2 + \sqrt{5}$ as well.]

(iii) $3 - \sqrt{5} = 2 + (1 - \sqrt{5})$ and $3 + \sqrt{5} = 2 \cdot 2 - (1 - \sqrt{5})$ so that $(3 - \sqrt{5}, 3 + \sqrt{5}) \subseteq (2, 1 - \sqrt{5})$. For the reverse inclusion, note that $(3 - \sqrt{5})(3 + \sqrt{5}) = 4$ is in $(3 - \sqrt{5}, 3 + \sqrt{5})$, so that $4 - (3 + \sqrt{5}) = 1 - \sqrt{5}$ is in it. Also $(3 + \sqrt{5}) + (3 - \sqrt{5}) = 6$ is in it, so $6 - 4 = 2$ is in it, which shows the reverse inclusion.

(i) For $(11) \subseteq (3 + 2\sqrt{5})$ we just have to show that $11 = (a + b\sqrt{5})(3 + 2\sqrt{5})$ for some a and b in $\mathbf{Z}$. Computing this using division we get that $11 = (-3 + 2\sqrt{5})(3 + 2\sqrt{5})$. To show that $(11) \neq (3 + 2\sqrt{5})$ we now have to show that $3 + 2\sqrt{5} \notin (11)$, i.e., we do not have $(a + b\sqrt{5})11 = 3 + 2\sqrt{5}$ for any a and b in $\mathbf{Z}$. This is clear as $11a = 3$ has no solution in $\mathbf{Z}$.

84. As $\mathbf{Z}[\sqrt{-5}]$ is a commutative ring with identity, we shall use Q.63 a lot to check two ideals are equal.

(i) $(1 - \sqrt{-5}, 2) \subseteq (1 + \sqrt{-5}, 2)$ as $1 - \sqrt{-5} = 1 \cdot (1 + \sqrt{-5}) + (-1) \cdot 2$, and $(1 + \sqrt{-5}, 2) \subseteq (1 - \sqrt{-5}, 2)$ as $1 + \sqrt{-5} = 1 \cdot (1 - \sqrt{-5}) + 1 \cdot 2$.

(i) As $(1) = \mathbf{Z}[\sqrt{-5}]$, we have $(2\sqrt{-5}, 3) \subseteq (1)$. Note that $\sqrt{-5} \cdot 2\sqrt{-5} = -10$ is in $(2\sqrt{-5}, 3)$, so $-10 + 3 \cdot 3 = 1$ is in it, hence $(1) \subseteq (2\sqrt{-5}, 3)$ as well.

(i) By Q.82, $(1 + \sqrt{-5}, 3) \cdot (1 - \sqrt{-5}, 2) = (6, 2 + 2\sqrt{-5}, 3 - 3\sqrt{-5}, 6)$. Note that then the element $(3 - 3\sqrt{-5}) - (2 + 2\sqrt{-5}) = 1 - 5\sqrt{-5}$ is in this ideal, so also $\sqrt{-5} \cdot 6 + (1 - 5\sqrt{-5}) = 1 + \sqrt{-5}$ is in this ideal. This shows that $(1 + \sqrt{-5}) \subseteq (2 + 2\sqrt{-5}, 3 - 3\sqrt{-5}, 6)$. For the reverse inclusion we need to show that $2 + 2\sqrt{-5}, 3 - 3\sqrt{-5}$ and 6 are in $(1 + \sqrt{-5})$. Clearly $2 + 2\sqrt{-5} = 2(1 + \sqrt{-5})$ and $6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ are in it. Then $3(1 + \sqrt{-5}) - \sqrt{-5} \cdot 6 = 3 - 3\sqrt{-5}$ is in $(1 + \sqrt{-5})$ as well. [Alternatively, we can check this by checking if $(2 + 2\sqrt{-5})/(1 + \sqrt{-5})$, $(3 - 3\sqrt{-5})/(1 + \sqrt{-5})$ and $6/(1 + \sqrt{-5})$ are in $\mathbf{Z}[\sqrt{-5}]$.]

(i) The manipulations here very similar to the previous part replacing $\sqrt{-5}$ with $-\sqrt{-5}$ everywhere.

(i) $(1 - \sqrt{-5}, 2)^2 = (-4 - 2\sqrt{-5}, 2 - 2\sqrt{-5}, 2 - 2\sqrt{-5}, 4)$ by Q.82. As we need each generator only once, this equals the ideal $(-4 - 2\sqrt{-5}, 2 - 2\sqrt{-5}, 4)$. This is contained in (2) as $-4 - 2\sqrt{-5} = (-2 - \sqrt{-5}) \cdot 2$ etc. Now we notice that $(2 - 2\sqrt{-5}) - (-4 - 2\sqrt{-5}) - 4 = 2$ is in $(-4 - 2\sqrt{-5}, 2 - 2\sqrt{-5}, 4)$ which shows that $(1 - \sqrt{-5}, 2)^2 \supseteq (2)$ as well.

(i) If $(1 - \sqrt{-5}, 2) = (\alpha)$ for some α in $\mathbf{Z}[\sqrt{-5}]$, so α divides both $1 - \sqrt{-5}$ and 2 in $\mathbf{Z}[\sqrt{-5}]$. Then $N(\alpha)$ must divide $N(1 - \sqrt{-5}) = 6$ and $N(2) = 4$ in $\mathbf{Z}$ so that $N(\alpha)$ divides 2. As $N(\alpha) \geq 0$, we must have $N(\alpha) = 1$ or 2. If $\alpha = a + b\sqrt{-5}$, $N(\alpha) = a^2 + 5b^2$ so there are only two possible α's, ± 1. As α and $-\alpha$ generate the same ideal, we can assume $\alpha = 1$ if necessary, and see if $(1 - \sqrt{-5}, 2) = (1) = \mathbf{Z}[\sqrt{-5}]$. But if that were the case, then $(1) = (1)^2 = (1 - \sqrt{-5}, 2)^2 = (2)$ from what we did before, so $1 = 2(c + d\sqrt{-5})$ for some c and d in $\mathbf{Z}$, which is not possible. So $(1 - \sqrt{-5}, 2)$ is not a principal ideal. [Alternatively, as generators of principal ideals in integral domains are unique up to units (check: in an integral domain R, $(a) = (b)$ if and only if $a = bu$ for some unit $u \in R^*$), we could argue as follows. If $(1 - \sqrt{-5}, 2) = (\alpha)$, then $(\alpha^2) = (\alpha)^2 = (1 - \sqrt{-5}, 2)^2 = (2)$ so that $2 = \pm\alpha^2$ as the units in $\mathbf{Z}[\sqrt{-5}]$ are ± 1. Then $2^2 = N(2) = N(\pm\alpha^2) = N(\pm 1)N(\alpha^2) = N(\alpha)^2$ so that $N(\alpha) = 2$ as $N(\alpha) \geq 0$. This is not possible as $a^2 + 5b^2 = 2$ has no solutions for a and b in $\mathbf{Z}$.]

85. In order to show that $I + J = \mathbf{Z}[i]$, we have to show that 1 is in $I + J$, as $\mathbf{Z}[i]$ has an identity. So we have to write $1 = \alpha + \beta$ with α in I and β in J. One way of doing that is using the Euclidean algorithm in $\mathbf{Z}[i]$ (see Q.45), computing the greatest common divisor of $3 - 2i$ and $3 + 2i$, and expressing it in the form $\alpha(3 - 2i) + \beta(3 + 2i)$. This gives $3 - 2i = -i(3 + 2i) + (1 + i)$, $3 + 2i = 2(1 + i) + 1$, and so $1 = (3 + 2i) - 2(1 + i) = (3 + 2i) - 2[(3 - 2i) + i(3 + 2i)] = -2(3 - 2i) + (1 - 2i)(3 + 2i)$. [Alternatively, you can find that 1 is in $I + J$ by playing around: $3 - 2i + 3 + 2i = 6$ is in $I + J$; $3 - 2i - (3 + 2i) = -4i$ is in $I + J$, and so is $i(-4i) = 4$; then $6 - 4 = 2$ is in $I + J$, and hence $3 + 2i - (1 + i)2 = 1$. Note that this approach only shows that 1 is in $I + J$, but does not express it in the form $\alpha + \beta$ with α in I and β in J, so this would not be enough for the last bit of the question.] Because $\mathbf{Z}[i]$ is commutative with identity, we have that $I \cap J = I \cdot J = (3 - 2i) \cdot (3 + 2i) = ((3 - 2i)(3 + 2i)) = (13)$. By the Chinese remainder theorem, $\mathbf{Z}[i]/(13) \cong \mathbf{Z}[i]/I \times \mathbf{Z}[i]/J = \mathbf{Z}[i]/(3 - 2i) \times \mathbf{Z}[i]/(3 + 2i)$. If $1 = \alpha + \beta$ with α in I and β in J, then the

element in $\mathbf{Z}[i]/(13)$ that maps to $(\overline{1},\overline{2})$ is given by $\overline{1\cdot\beta+2\cdot\alpha}$. With the α and β found before, we get $1\cdot(1-2i)(3+2i)+2\cdot(-2(3-2i))=-5+4i$.

86. Let $I=(X+1)$ and $J=(X^2+2)$, which are ideals in $\mathbf{Q}[X]$. Then $I+J=\mathbf{Q}[X]$: $\mathbf{Q}[X]$ is commutative with identity, so we only have to write $1=f(X)(X+1)+g(X)(X^2+2)$ for some $f(X)$ and $g(X)$ in $\mathbf{Q}[X]$, and we can find such $f(X)$ and $g(X)$ using the Euclidean algorithm as in Theorem 2.13. We get that $1=\frac{1}{3}(1-X)(X+1)+\frac{1}{3}(X^2+2)$. Then by the Chinese remainder theorem, because $\mathbf{Q}[X]$ is commutative with identity, $I\cap J=I\cdot J=(X+1)\cdot(X^2+2)=((X+1)(X^2+2))=(X^3+X^2+2X+2)$, and we get an isomorphism $\mathbf{Q}[X]/(X^3+X^2+2X+2)\cong\mathbf{Q}[X]/I\times\mathbf{Q}[X]/J=\mathbf{Q}[X]/(X+1)\times\mathbf{Q}[X]/(X^2+2)$. The element mapping to $(\overline{X},\overline{2X})$ is given by $\overline{X\frac{1}{3}(X^2+2)+2X\frac{1}{3}(1-X)(X+1)}=\overline{-\frac{1}{3}X^3+\frac{4}{3}X}$.

87. We write $1=X+(-(X-1))$ so that as ideals $(X)+(X-1)=\mathbf{Q}[X]$. So by the Chinese remainder theorem we get that $(X)\cap(X-1)=(X)\cdot(X-1)=(X^2-X)$ as $\mathbf{Q}[X]$ is a commutative ring with 1, and $\mathbf{Q}[X]/(X^2-X)\cong\mathbf{Q}[X]/(X)\times\mathbf{Q}[X]/(X-1)$ under the natural map. Then $3=3X+(-3)(X-1)$ and $5=5X+(-5)X$ so that we should take $(-3)(X-1)+5X=2X+3$ in $\mathbf{Q}[X]$: $\overline{2X+3}$ in $\mathbf{Q}[X]/(X^2-X)$ maps to $(\overline{3},\overline{5})$ in $\mathbf{Q}[X]/(X)\times\mathbf{Q}[X]/(X-1)$.

88. The idea is to show that (X^2-5) is a maximal ideal in $\mathbf{Q}[X]$ (a commutative ring with identity $1\neq 0$), and that $\mathbf{Q}[X]/(X^2-5)\cong\mathbf{Q}[\sqrt{5}]$ as rings, because then $\mathbf{Q}[X]/(X^2-5)$ is a field by Theorem 3.25, and so $\mathbf{Q}[\sqrt{5}]$ is a field because it is isomorphic to $\mathbf{Q}[X]/(X^2-5)$ as rings. X^2-5 is irreducible in $\mathbf{Q}[X]$ as it is of degree two, but has no roots in $\mathbf{Q}$: the candidates for roots in $\mathbf{Q}$ would be ±1 and ±5, and none of these are roots. Hence, since all maximal ideals in $\mathbf{Q}(X)$ are of the form $\big(f(X)\big)$ for some *irreducible* polynomial $f(X)$, (X^2-5) is a maximal ideal in $\mathbf{Q}[X]$, and as $\mathbf{Q}[X]$ is a commutative ring with identity $1\neq 0$, the quotient $\mathbf{Q}[X]/(X^2-5)$ is a field, again by Theorem 3.25.

In order to show that $\mathbf{Q}[X]/(X^2-5)\cong\mathbf{Q}[\sqrt{5}]$, we try to define a surjective ring homomorphism $\varphi:\mathbf{Q}[X]\to\sqrt{5}$ with $\mathrm{Ker}\,(\varphi)=(X^2-5)$, so that we can apply the first isomorphism theorem for rings. So once we've done this, we are done. $\mathbf{Q}[\sqrt{5}]=\{a+b\sqrt{5}$ with a,b in $\mathbf{Q}\}$, a subring of $\mathbf{C}$. Define $\varphi:\mathbf{Q}[X]\to\mathbf{Q}[\sqrt{5}]$ via $f(X)=f(\sqrt{5})$. Note that $f(\sqrt{5})$ is in $\mathbf{Q}[\sqrt{5}]$ because any term $a(\sqrt{5})^n$ with a in $\mathbf{Q}$ and $n\geq 0$ will be of the form b or $b\sqrt{5}$ for some rational number b.

φ is a homomorphism of rings by the specialisation homomorphism as $\mathbf{Q}$ is clearly a subring of $\mathbf{Q}[\sqrt{5}]$.

φ is surjective, as for a and b in $\mathbf{Q}$, $\varphi(bX+a)=a+b\sqrt{5}$, so we get all elements in $\mathbf{Q}[\sqrt{5}]$.

In order to determine $\mathrm{Ker}\,(\varphi)$, first notice that $(X^2-5)\subseteq\mathrm{Ker}\,(\varphi)$: elements in (X^2-5) are of the form $f(X)(X^2-5)$ for some $f(X)$ in $\mathbf{Q}[X]$, and then $\varphi(f(X)(X^2-5))=\varphi(f(X))\varphi(X^2-5)=\varphi(f(X))0=0$. To see $\mathrm{Ker}\,(\varphi)\subseteq(X^2-5)$ as well, we could go about it in two ways. The quick way is to notice that we know that $(X^2-5)\subseteq\mathrm{Ker}\,(\varphi)\subseteq\mathbf{Q}[X]$, and we know that (X^2-5) is a maximal ideal in $\mathbf{Q}[X]$. So from the definition of maximal ideals, either $\mathrm{Ker}\,(\varphi)=(X^2-5)$ or $\mathrm{Ker}\,(\varphi)=\mathbf{Q}[X]$. The last cannot happen as that would mean that $\varphi(1)=0$ which is clearly not the case. The other way of seeing it is more computational: if $g(X)$ is in $\mathrm{Ker}\,(\varphi)$, write $g(X)=h(X)(X^2-5)+(aX+b)$ with a and b in $\mathbf{Q}$ by using long division in $\mathbf{Q}[X]$. Because φ is a homomorphism or rings, and $g(X)$ is in $\mathrm{Ker}\,(\varphi)$, $0=\varphi(g(X))=\varphi(h(X))\varphi(X^2-5)+\varphi(aX+b)=b+a\sqrt{5}$, so $a=b=0$ and $g(X)=h(X)(X^2-5)$ lies in (X^2-5). So $\mathrm{Ker}\,(\varphi)\subseteq(X^2-5)$ as well, and equality must hold: $\mathrm{Ker}\,(\varphi)=(X^2-5)$.

Either way, we can now apply the first isomorphism theorem for rings: $\mathbf{Q}[X]/(X^2-5)\cong\mathbf{Q}[\sqrt{5}]$ as rings.

89. We would be tempted to use the map $f(X)\mapsto f(i\sqrt{3})$, but that will not map X^2+X+1 to zero. Instead, we use one of the roots of X^2+X+1, like $\alpha=(-1-i\sqrt{3})/2$. So we define $\varphi:\mathbf{Q}[X]\to\mathbf{C}$ by $\varphi(f(X))=f(\alpha)$. This is a ring homomorphism, as it is a specialisation homomorphism. We first determine its kernel. As α is root of X^2+X+1, if $f(X)=g(X)(X^2+X+1)$ is in (X^2+X+1), $\varphi(f(X))=\varphi(g(X))\varphi(X^2+X+1)=0$ so that $(X^2+X+1)\subseteq\mathrm{Ker}\,(\varphi)$. Conversely, if $f(X)$ is in $\mathrm{Ker}\,(\varphi)$, we can write $f(X)=q(X)(X^2+X+1)+aX+b$ for some $q(X)$ in $\mathbf{Q}[X]$ and a, b in $\mathbf{Q}$ (use division with remainder). Then $0=\varphi(f(X))=a\alpha+b$. If $a\neq 0$, we would get $\alpha=-b/a$ would be in $\mathbf{R}$ (or even $\mathbf{Q}$), which is clearly not the case. So $a=0$ and hence $b=0$. therefore $f(X)=q(X)(X+X+1)$ lies in (X^2+X+1) and $\mathrm{Ker}\,(\varphi)=(X^2+X+1)$. In order to determine the image of φ, $\Im(\varphi)$, write any $f(X)$ in $\mathbf{Q}[X]$ as $q(X)(X^2+X+1)+aX+b$ with $q(X)$ in $\mathbf{Q}[X]$ and a, b

in $\mathbf{Q}$ (use again division with remainder). Then $\varphi(f(X)) = a\alpha + b = (b - \frac{a}{2}) - \frac{a}{2}i\sqrt{3}$ lies in $\mathbf{Q}[i\sqrt{3}]$. Also $\varphi(-2bX + (a-b)) = a + bi\sqrt{3}$ for a, b in $\mathbf{Q}$ so that φ is surjective. So by the first isomorphism theorem we get an isomorphism $\mathbf{Q}[X]/(X^2+X+1) \cong \mathbf{Q}[i\sqrt{3}]$. Now in order to show that $\mathbf{Q}[i\sqrt{3}]$ is a field, we use Theorem 3.25 and since all maximal ideals in $\mathbf{Q}(X)$ are of the form $\big(f(X)\big)$ for some *irreducible* polynomial $f(X)$. By the latter, (X^2+X+1) is a maximal ideal in $\mathbf{Q}[X]$ as X^2+X+1 is irreducible in $\mathbf{Q}[X]$: it is of degree two but does not have any roots in $\mathbf{Q}$ (or even $\mathbf{R}$). Because $\mathbf{Q}[X]$ is a commutative ring with identity $1 \neq 0$, Theorem 3.25 tells us that $\mathbf{Q}[X]/(X^2+X+1)$ must be a field.

90. We define a map $\mathbf{Z}[X] \to \mathbf{Z}_n$ by mapping $f(X)$ to $\overline{f(0)}$. This is the composition of the maps $\mathbf{Z}[X] \to \mathbf{Z}$ given by $f(X) \mapsto f(0)$, and $\mathbf{Z} \to \mathbf{Z}_n$ given by $a \mapsto \overline{a}$. both those maps are (specialisation) homomorphisms of rings, and so is their composition. Alternatively, it is easy to write it out starting with $f(X)$ and $g(X)$ in $\mathbf{Z}[X]$. If $f(X)$ lies in (X,n), $f(X) = g(X)X + h(X)n$ for some $g(X)$ and $h(X)$ in $\mathbf{Z}[X]$. Then $\varphi(f(X)) = \overline{g(0)0 + h(0)n} = \overline{0}$, so $(X,n) \subseteq \mathrm{Ker}\,(\varphi)$. To show the reverse inclusion, take $f(X)$ in $\mathrm{Ker}\,(\varphi)$, and write it as $g(X)X + m$ where m is the constant term of $f(X)$. Then $f(0) = m$. As $\varphi(f(X)) = \overline{0}$, m is divisible by n, say $m = kn$ for some k in $\mathbf{Z}$. Then $f(X) = g(X)X + kn$ lies in (X,n). This shows that $\mathrm{Ker}\,(\varphi) = (X,n)$.

φ is surjective as $0, 1, \ldots, n-1$ map to $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. So by the first isomorphism theorem, we get an isomorphism $\mathbf{Z}[X]/(X,n) \cong \mathbf{Z}_n$. As $\mathbf{Z}[X]$ is a commutative ring with identity $1 \neq 0$, Theorem 3.25 tells us that (X,n) is a prime (resp. maximal) ideal if and only if $\mathbf{Z}_n$ is an integral domain (resp. a field). By Example 3.24, this happens if and only if n is a prime number.

91. For the first we'll give two answers: one directly from the definitions, and one using more theory.

(X) consists of the polynomials with vanishing constant term. If $f(X)g(X)$ lies in (X), either $f(X)$ of $g(X)$ must have vanishing constant term (because $\mathbf{Z}$ is an integral domain), so lies in (X). This means (X) is a prime ideal. It cannot be maximal: $(X,2)$ is certainly a larger ideal as it contains 2. It is also not the whole of $\mathbf{Z}[X]$: $1 = f(X)X + g(X)2$ leads to a contradiction by looking at the constant term. So we have $(X) \subset (X,2) \subset \mathbf{Z}[X]$ with the inclusions strict, and (X) is not maximal.

We can get a quick answer by using the first isomorphism theorem as in Q.90.

One shows that $\mathbf{Z}[X]/(X) \cong \mathbf{Z}$ and $\mathbf{Z}[X]/(n) \cong \mathbf{Z}_n[X]$. (The maps to use are $\varphi : \mathbf{Z}[X] \to \mathbf{Z}$ given by $\varphi(f(X)) = f(0)$ and $\psi : \mathbf{Z}[X] \to \mathbf{Z}_n[X]$ given by $\psi(f(X)) = \overline{f}(X)$, i.e., reduction of the coefficients modulo n. φ is a ring homomorphism (simply write it out or use that it is a specialisation homomorphism), and ψ is a ring homomorphism (reduction of coefficients).) As $\mathbf{Z}[X]$ is a commutative ring with identity $1 \neq 0$ we only have to see if $\mathbf{Z}$ or $\mathbf{Z}_n[X]$ are integral domains and/or fields by Theorem 3.25, $\mathbf{Z}$ is an integral domain but not a field, so (X) is a prime ideal in $\mathbf{Z}[X]$ but not a maximal ideal. For $\mathbf{Z}_n[X]$ it depends on n. If n is *not* a prime number, $\mathbf{Z}_n$ is not an integral domain by Example 3.24. Then $\mathbf{Z}_n[X]$ (which contains $\mathbf{Z}_n$ as the constants) cannot be an integral domain, and certainly not a field, so (n) is neither a prime ideal nor a maximal ideal in $\mathbf{Z}[X]$ in this case. If n *is* a prime number, $\mathbf{Z}_n$ is a field by Example 3.24, and $\mathbf{Z}_n[X]$ is an integral domain in this case (degrees add up for a product of polynomials). But it is not a field by Q.32 as not every nonzero element of $\mathbf{Z}_n[X]$ is a unit. So now (n) is a prime ideal but not a maximal ideal in $\mathbf{Z}[X]$. [That (n) is not a maximal ideal in $\mathbf{Z}[X]$ can be seen by hand: (n,X) contains (n) but is not equal to it as (n) consists of all elements in $\mathbf{Z}[X]$ with *all* coefficients divisible by n and X is not of this shape. Also $(n,X) \neq \mathbf{Z}[X]$ because otherwise we could write $1 = f(X)n + g(X)X$ for some $f(X)$ and $g(X)$ in $\mathbf{Z}[X]$, and as $n \geq 2$ this is impossible by looking at the constant term.]

92. All rings are commutative with nonzero identity, so we can apply Theorem 3.25 directly, as the quotient rings are identified in the Exercises. This gives us that $(-4+i)$ is a maximal ideal (and hence a prime ideal) in $\mathbf{Z}[i]$ as $\mathbf{Z}_17$ is a field because 17 is prime, and $\mathbf{Z}[i]/(-4+i) \cong \mathbf{Z}_{17}$. $(2, 1+\sqrt{5})$ is maximal (and hence prime) in $\mathbf{Z}[\sqrt{5}]$ because $\mathbf{Z}_2$ is a field as 2 is prime, and $\mathbf{Z}[\sqrt{5}]/(2, 1+\sqrt{5}) \cong \mathbf{Z}_2$. $(9, 4-\sqrt{7})$ is not a prime ideal in $\mathbf{Z}[\sqrt{7}]$ because $\mathbf{Z}[\sqrt{7}]/(9.4-\sqrt{7}) \cong \mathbf{Z}_9$ and 9 is not prime, so $\mathbf{Z}_9$ is not an integral domain. Hence $(9, 4-\sqrt{7})$ is not a maximal ideal either. (of course, this also follows because $\mathbf{Z}_9$ is not a field.) $(X+1)$ is a maximal ideal in $\mathbf{Z}_3[X]$ because $\mathbf{Z}_3[X]/(X+1) \cong \mathbf{Z}_3$ which is a field as 3 is prime, and hence it is also a prime ideal in $\mathbf{Z}_3[X]$. With $\mathbf{Q}[X]/(X^2-2)$ we can argue both ways. Either we say that X^2-2 is irreducible in $\mathbf{Q}[X]$ because X^2-2 is of degree 2 and has no rational roots, therefore, since all maximal ideals in $\mathbf{Q}(X)$ are of the form $\big(f(X)\big)$ for some *irreducible* polynomial $f(X)$, we conclude that (X^2-2) is maximal and

(consequently) prime. So then it follows that $\mathbf{Q}[\sqrt{2}]$ is a field. We could also check by hand that $\mathbf{Q}[\sqrt{2}]$, which is a subring of $\mathbf{C}$ by Q.12 is a field. (See Q.21.) Then we can conclude that $(X^2 - 2)$ is a maximal ideal (hence a prime ideal) in $\mathbf{Q}[X]$ as $\mathbf{Q}[X]/(X^2 - 2)$ is isomorphic to the field $\mathbf{Q}[\sqrt{2}]$, so must be a field itself.