SECTION A

1. An element $r \in R$ is a unit if there exists $s \in R$ with $rs = 1$.

(i) $(-1)^2 = 1$ so $-1 \in \mathbf{Z}$ is a unit.

(ii) $5 \times 3 = 1$ so $5 \in \mathbf{Z}/7\mathbf{Z}$ is a unit.

(iii) $5 \times 5 = 1$ so $5 \in \mathbf{Z}/8\mathbf{Z}$ is a unit.

(iv) $x^2 + 1$ is not a unit in $\mathbf{Z}[x]$ because the product of $x^2 + 1$ with another polynomial is either 0 or a polynomial of degree ≥ 2 and in particular is therefore not 1.

(v) $1 + i$ is not a unit in $\mathbf{Z}[i]$ because $|1 + i|^2 = 2$ and so

$$|(1 + i)(a + bi)|^2 = 2(a^2 + b^2) \neq 1$$

for any $a, b \in \mathbf{Z}$.

2. A non-zero element $r \in R$ is irreducible if we cannot write $r = st$ for two non-units $s, t \in R$.

(i) $f(x) = x^3 + 2x^2 + x + 2$ is not irreducible because $f(2) = 0$ and we have $f(x) = (x - 2)(x^2 + 4x - 1)$.

(ii) $f(x) = x^4 + x - 1$ has no linear factors because it has no roots in $\mathbf{Z}$: $f(0), f(\pm 1) \neq 0$ and if $|n| > 1$ then $f(n) > 12$. Since the coefficient of x^4 is 1 and the constant term is -1 the only possible factorisation into quadratics is of the form

$$x^4 + x - 1 = (x^2 + ax + 1)(x^2 + bx - 1).$$

Comparing coefficients we find that

$$a + b = 0,\ ab = 0,\ b - a = 1.$$

There are no solutions to these equations and so no possible factorisation; $f(x)$ is irreducible in $\mathbf{Z}[x]$.

(iii) If $f(x) = x^4 + x - 1$ then $f(0) = -1$ and $f(1) = 1$ so there is a real root between 0 and 1 (by the intermediate value theorem). Hence $f(x)$ is not irreducible in $\mathbf{R}[x]$.

3. The elements of $(\mathbf{Z}/2\mathbf{Z})[x]/\langle x^2+x+1\rangle$ are $0, 1, x, 1+x$ (in standard form).

The multiplication table is

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

R is a field because each non-zero element has a multiplicative inverse — there is a 1 in each non-zero row and column.

(It is also acceptable for them to note that x^2+x+1 is irreducible and quote the result which says that the quotient by an ideal generated by an irreducible is a field.)

4. We use the Euclidean algorithm.

$$\frac{5}{1+3i} = -i + \left(\frac{1}{2} - \frac{i}{2}\right)$$

so that $5 = -i(1+3i) + (2+i)$ with $|2+i|^2 = 5 < 10 = |1+3i|^2$.

Then

$$\frac{1+3i}{2+i} = 1+i$$

so that the greatest common divisor is the last non-zero remainder i.e.

$$g = 2+i.$$

We have $\frac{5}{2+i} = 2-i$ so that $a = 2-i$ and $\frac{1+3i}{2+i} = 1+i$ so that $b = 1+i$.

Finally $g = 2+i = 5+i(1+3i)$ so $c = 1$ and $d = i$.

5. A t-(v,k,r)-design consists of a set X of size v together with a collection B of subsets of X (the blocks), each of size k, with the property that each subset of r elements of X occurs in precisely t blocks.

a) The subsets of size 2 in a set of size 5 form a 1-$(5,2,4)$-design because each element occurs in exactly 4 subsets of size 2 (there are 4 other elements with which it can be paired).

b) The lines in the 7 point projective plane $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$ form a 2-$(7,3,1)$-design: there are 3 points on each line and each pair of points lies on a unique line.

6. a) The length of the code is the number of columns of the check matrix M, in this case 7. The dimension of the code is the length minus the number of linearly independent rows of the check matrix, in this case $7 - 3 = 4$. Since no column is identically zero and no two are the same the weight is ≥ 3.

The number of words in the code is $2^4 = 16$ i.e. the number of elements in a linear subspace of $(\mathbf{Z}/2\mathbf{Z})^7$ of dimension 4. Since the weight is ≥ 3 at least one error can be corrected.

b)

(i) Since $M(1110001)^T = (000)^T$ the word 1110001 is in C.

(ii) Since $M(1101110)^T = (110)^T$ the word 1110001 is not in C. Since $(110)^T$ is the fourth column of M the fourth entry of the word is incorrect and so the corrected word is

1100110

(which is in the code).

SECTION B

7. A ring homomorphism from R to S is a map $\varphi : R \to S$ such that

- $\varphi(r - r') = \varphi(r) - \varphi(r') \qquad \forall r, r' \in R$;
- $\varphi(rr') = \varphi(r)\varphi(r') \qquad \forall r, r' \in R$;
- $\varphi(1) = 1$.

(Note the last condition; this was the course's convention since it dealt with rings with multiplicative identity.)

(i) $\varphi : \mathbf{Z} \to \mathbf{Z}/6\mathbf{Z} : m \mapsto m \bmod 6$ is a ring homomorphism (standard check). The kernel is $6\mathbf{Z}$.

(ii) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto m^2$ is not a ring homomorphism because, for example, $(1+1)^2 = 4 \neq 1^2 + 1^2$.

(iii) $\varphi : \mathbf{Q}[x] \to \mathbf{Q} : p(x) \mapsto p(3)$ is a ring homomorphism (standard check). It is also acceptable for them to quote the result that evaluation maps from polynomial rings are always homomorphisms.

The kernel is the subset of polynomials with 3 as a root or, equivalently, the polynomials with $x - 3$ as a factor. (Either formulation is acceptable.)

(iv) $\varphi : (\mathbf{Z}/2\mathbf{Z})[x] \to (\mathbf{Z}/2\mathbf{Z})[x] : p(x) \mapsto p(x)^2$ is a ring homomorphism. Suppose $p(x) = a_0 + a_1 x + \ldots a_n x^n$. Then

$$p(x)^2 = (a_0^2 + a_1^2 x^2 + \ldots + a_n^2 x^{2n}) + 2 \times (\text{cross terms}) = p(x^2)$$

because $a^2 = a$ in $\mathbf{Z}/2\mathbf{Z}$. It easily follows that φ is a ring homomorphism.

The kernel is $\{0\}$.

8. a) Elements of the quotient ring correspond to polynomials in R of degree < 4 so there are $2^4 = 16$ of them. Since $f(x)$ is irreducible $(R/I)^* = R/I - \{0\}$ and so has 15 elements. The possible orders of elements are the divisors of 15 i.e. $1, 3, 5$ and 15.

b) Clearly $x + 1$ doesn't have order 1 and

$$(x+1)^5 = (x+1)(x+1)^4 = (x+1)(x^4+1) = (x+1)x^3 = 1$$

so $x + 1$ has order 5 in $(R/I)^*$.

Clearly $x^3 + x$ doesn't have order 1 and

$$(x^3+x)^2 = x^2(x^4+1) = x^5 = x(x^3+1) = x^3 + x + 1$$

so

$$(x^3+x)^3 = (x^3+x)(x^3+x+1) = x^6 + x^3 + x^2 + x = x^5 + x^3 + x = x^4 + x^3 = 1.$$

Hence $x^3 + x$ has order 3 in $(R/I)^*$.

c) We have $(x+1)(x^3+x) = x^4 + x^3 + x^2 + x = x^2 + x + 1$ in standard form. Clearly $x^2 + x + 1$ doesn't have order 1. It can't have order 3 because

$$(x+1)^3(x^3+x)^3 = (x+1)^3 \neq 1$$

nor can it have order 5 because

$$(x+1)^5(x^3+x)^5 = (x^3+x)^5 \neq 1.$$

The only remaining possibility is that $x^2 + x + 1$ has order 15.

9. a) Clearly $\sqrt{2}$ is a root of x^2-2 which is irreducible in $\mathbf{Z}[x]$ because 2 is not a perfect square. Hence, by Gauss's lemma, x^2-2 is irreducible in $\mathbf{Q}[x]$ and so is the minimal polynomial of $\sqrt{2}$.

Let $\alpha = \sqrt{2}+\sqrt{7}$. Then $\alpha^2 = 9+2\sqrt{14}$ so

$$(\alpha^2-9)^2 = 56 \quad \text{or, equivalently,} \quad \alpha^4 - 18\alpha^2 + 25 = 0.$$

We have $\alpha(\alpha^2-9) = (\sqrt{2}+\sqrt{7})2\sqrt{14} = 4\sqrt{7}+14\sqrt{2}$. Hence

$$\alpha(\alpha^2-9) - 4\alpha = 10\sqrt{2}$$

or, equivalently,

$$\sqrt{2} = \frac{1}{10}\Big(\alpha(\alpha^2-9) - 4\alpha\Big) \in \mathbf{Q}[\alpha].$$

b)

(i) Since the minimal polynomial of $\sqrt{2}$ has degree 2 we have $[\mathbf{Q}[\sqrt{2}] : \mathbf{Q}] = 2$.

(ii) Since $\sqrt{2} \in \mathbf{Q}[\alpha]$ we deduce that so is $\sqrt{7} = \alpha - \sqrt{2}$. We are told that $\sqrt{7} \notin \mathbf{Q}[\sqrt{2}]$ so that $[\mathbf{Q}[\alpha] : \mathbf{Q}[\sqrt{2}]] \geq 2$. Since $\sqrt{7}$ satisfies a quadratic in $\mathbf{Q}[\sqrt{2}][x]$ we must have $[\mathbf{Q}[\alpha] : \mathbf{Q}[\sqrt{2}]] = 2$.

(iii) By the above $[\mathbf{Q}[\alpha] : \mathbf{Q}] = [\mathbf{Q}[\alpha] : \mathbf{Q}[\sqrt{2}]] \times [\mathbf{Q}[\sqrt{2}] : \mathbf{Q}] = 2 \times 2 = 4$.

10. a) There are four sets of parallel lines in $\mathbf{Z}_3^2$ namely,

$$x + c = 0, \quad y + c = 0, \quad x + y + c = 0, \quad x + 2y + c = 0$$

where $c = 0, 1$ or 2. The tasters correspond to these different values of c. The ice-creams correspond to the 9 points in $\mathbf{Z}_3^2$. The schedule is then as follows, where 1 indicates that an ice-cream is tested by the taster, and 0 indicates that it is not.

	$(0,0)$	$(1,0)$	$(2,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(0,2)$	$(1,2)$	$(2,2)$
Session 1	.	.	.	.	.	.	.	.	.
$x = 0$	1	0	0	1	0	0	1	0	0
$x + 1 = 0$	0	0	1	0	0	1	0	0	1
$x + 2 = 0$	0	1	0	0	1	0	0	1	0
Session 2	.	.	.	.	.	.	.	.	.
$y = 0$	1	1	1	0	0	0	0	0	0
$y + 1 = 0$	0	0	0	0	0	0	1	1	1
$y + 2 = 0$	0	0	0	1	1	1	0	0	0
Session 3	.	.	.	.	.	.	.	.	.
$x + y = 0$	1	0	0	0	0	1	0	1	0
$x + y + 1 = 0$	0	0	1	0	1	0	1	0	0
$x + y + 2 = 0$	0	1	0	1	0	0	0	0	1
Session 4	.	.	.	.	.	.	.	.	.
$x + 2y = 0$	1	0	0	0	1	0	0	0	1
$x + 2y + 1 = 0$	0	0	1	1	0	0	0	1	0
$x + 2y + 2 = 0$	0	1	0	0	0	1	1	0	0

b) There is a field $\mathbf{F}$ with $4 = 2^2$ elements. The plane $\mathbf{F}^2$ has $4^2 = 16$ elements and there are $(4^2 - 1)/(4 - 1) = 5$ sets of parallel lines

$$\{ax + by + c = 0 : c \in \mathbf{F}\}$$

for different choices of $(a, b) \neq (0, 0)$. This is obtained by counting the number of pairs $(a, b) \in \mathbf{F}^2$ with $(a, b) \neq (0, 0)$ up to a non-zero multiple, that is, if we count (a, b) then we do not count $\lambda(a, b)$ for $\lambda \neq 1$. As before, we would take the tasters corresponding to the values of c, the sessions corresponding to the sets of parallel lines, and the ice-creams corresponding to the points in $\mathbf{F}^2$.

11. a) The irreducible degree 2 polynomial in $(\mathbf{Z}/2\mathbf{Z})[x]$ is x^2+x+1, and the three irreducible degree 4 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$ are

$$x^4+x^3+x^2+x+1, \quad x^4+x+1 \quad \text{and} \quad x^4+x^3+1.$$

The theory of factorisations of $x^{p^n}-x$ in $(\mathbf{Z}/p\mathbf{Z})[x]$ tells us that the factors of $x^{16}+x$ in $(\mathbf{Z}/2\mathbf{Z})[x]$ are the irreducible polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$ of degrees dividing 16, and that each occurs once in the factorisation. Hence

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x+1)(x^4+x^3+1).$$

b) If $g(x)=(x+1)(x^4+x+1)$ then $g(x)h(x)=x^{15}+1$ where

$$\begin{aligned} h(x) &= (x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1) \\ &= x^{10}+x^9+x^8+x^6+x^5+x^2+1. \end{aligned}$$

The first row of the check matrix is the coefficients of $h(x)$ in descending order starting with that of the highest power x^{10} and followed by 4 zeros (to make 15 entries). The next row is the cyclic shift of this right by one place and so on. So the matrix is

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

There are no zero columns and no two columns are the same so the code has weight ≥ 3.

c) The number of cyclic codes of length 15 with dimension 7 corresponds to the number of factors of $x^{15}+1$ in $(\mathbf{Z}/2\mathbf{Z})[x]$ of degree 8. Such a factor consists of the product of two of the three distinct degree 4 factors. So there are 3 such codes.

The number of cyclic codes of length 15 with dimension 8 corresponds to the number of factors of $x^{15}+1$ in $(\mathbf{Z}/2\mathbf{Z})[x]$ of degree 7. Such a factor consists of the product of the degree 1 and 2 factors and one of the three distinct degree 4 factors. So there are again 3 such codes.