Solutions for January exam

1. A zero-divisor in a ring R is an element $r \in R$ such that $r \neq 0$ and there is an $s \neq 0 \in R$ such that $rs = 0$. [lecture] (1 mark)
   (a) $3 + 4i$ is not a zero-divisor in $\mathbf{Z}[i]$ because $\mathbf{Z}[i]$ is a subring of $\mathbf{C}$, which has no zero-divisors. (Arguments involving norms are equally acceptable.) [lecture] (2 marks)
   (b) 4 is not a zero-divisor in $\mathbf{Z}/15$ because $\gcd(4, 15) = 1$. (Or by listing all possibilities.) [lecture] (2 marks)
   (c) x is a zero-divisor in $\mathbf{Q}[x]/(x^2)$ because $x \cdot x = x^2 = 0$ in this ring. [similar to lecture] (2 mark)
   (d) 9 is a zero-divisor in $\mathbf{Z}/12$ because $9 \cdot 4 = 0$ in $\mathbf{Z}/12$. (Or because $\gcd(9, 12) > 1$.) [similar to lecture] (2 marks)

2a. The norm of 5 in $\mathbf{Z}[i]$ is 25, so we try to factor it as a product of two elements of norm 5. Noticing that $1 + 2i$ has norm 5, we try to divide 5 by $1 + 2i$ and get $5 = (1 + 2i)(1 - 2i)$. The factors are both irreducible, because their norms are prime. (It is acceptable to use associates of these factors.) [similar to lecture and homework] (3 marks)

2b. Trying values for x, we get the root $x = 2$, so $x + 3$ divides $x^3 + 4x + 4$. We find $x^3 + 4x + 4 = (x + 3)(x^2 + 2x + 3)$, and by direct trial the second factor has no roots, so it is irreducible. The factorization is $(x + 3)(x^2 + 2x + 3)$. [lecture and homework] (3 marks)

2c. This polynomial reduces mod 2 to $x^3 + x + 1$, which has no roots and is therefore irreducible. The polynomial must then be irreducible over $\mathbf{Q}$. Plainly it is not a multiple of any integer greater than 1, so the irreducible factorization is $x^3 + 5x - 105$. (3 marks)

3a. A field is a ring in which every element other than 0 is a unit (or, has a multiplicative inverse). [lecture] (3 marks)

3b. The elements are $0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$ (all polynomials in x whose degree is less than that of $x^3 + x + 1$).

To prove that it is a field, we must show that every element other than 0 is a unit. One sees that $1 \cdot 1 = 1$, so that 1 is a unit; that $x \cdot (x^2 + 1) = 1$, so that x and $x^2 + 1$ are units; that $(x + 1) \cdot (x^2 + x + 1) = 1$; so that $x + 1$ and $x^2 + x + 1$ are units; and finally that $x^2 \cdot (x^2 + x) = 1$, so that x^2 and $x^2 + x$ are units. [similar to homework] (6 marks)

4a. Adding the equations, we get $2y = 0$. Combining this with the equation $2x + z = 0$, we see that the variable z is free, so the general solution is $(t, 0, t)$. This gives the projective point $(1 : 0 : 1)$ (or $(2 : 0 : 2)$). [lecture and homework] (3 marks)

4b. If the line is $ax + by + cz = 0$, then we have $4b + c = 0$ and $3a + b + 2c = 0$. Thus $b = c$ and $a = -c$, giving a general solution of $(-t, t, t)$. The line could be $4x + y + z = 0$ (or any of three other possible equations for the same line). [similar to lecture and homework] (4 marks)

5. A t-(v, k, r)-design is a set of subsets T_i of size k of a set S of size v such that each t-element subset of S is a subset of exactly r of the T_i. [lecture] (3 marks)

5a. There are many possibilities, such as $(1, 2, 3), (4, 5, 6), (1, 3, 5), (2, 4, 6)$. [lecture and homework] (2 marks)

5b. There are 6 pairs of elements in a 4-element set, and 3 in a 3-element set, so if each pair is to appear twice there must be 4 subsets of order 3. But a set of order 4 has exactly 4 subsets with 3 elements, so this must be the design: $(1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4)$. [lecture and homework] (4 marks)

6i. The rank of the check matrix is 3, as is seen by adding the first row to the second and then the second to the third to put the matrix in echelon form. This code has dimension $5 - 3 = 2$ and its information rate is therefore $2/5$. [similar to lecture and homework] (4 marks)

6ii. We multiply the check matrix by the column vectors 01211 and 21110, getting respectively 000 and 001. So the first word is in the code and the second is not. [lecture and homework] (3 marks)

6iii. 001 is the third column of the matrix, so the corrected word is $21110 - 00100 = 21010$. [lecture and homework] (3 marks)

7. A ring homomorphism is a function ϕ from a ring R to a ring S such that $\phi(1) = 1$ and for all $r, r' \in R$ we have $\phi(r) + \phi(r') = \phi(r + r')$ and $\phi(r)\phi(r') = \phi(rr')$. [lecture] (3 marks)

7a. Not a homomorphism, because $\phi(1) + \phi(2) = 3 \neq \phi(1 + 2) = \phi(0) = 0$, or because $\phi(2)\phi(2) = 4 \neq \phi(2 \cdot 2) = \phi(1) = 1$. [similar to lecture and homework] (3 marks)

7b. Evaluation of polynomials gives a homomorphism. [lecture] (3 marks)

7c. This is the quotient map by (3), so it is a homomorphism. (3 marks) [lecture and homework]

7d. This is not a homomorphism, because $\phi(1) \neq 1$. [lecture and homework] (3 marks)

8. An ideal is a nonempty subset of a ring such that, for all $a, b \in I$ and $r \in R$, we have $a - b \in I$ and $ar \in I$. (There are minor variations of this definition that are equally acceptable.) (3 marks) [lecture]

8a. This is not an ideal, because (for example) it contains i but not $-1 \cdot i$. [similar to lecture and homework]

8b. This is an ideal. (The easiest way to show this is simply to point out that it is the set of multiples of x^2.) (3 marks) [similar to lecture and homework]

8c. Not an ideal, because $1 \in I$ and $\pi \in \mathbf{R}$ but $1 \cdot \pi \notin \mathbf{R}$. (3 marks) [lecture]

8d. This is an ideal. Again, the easiest way to show this is to notice that it is the set of multiples of $x - 1$, but it is also a basic fact in the theory of cyclic codes. (3 marks) [lecture]

9i. The elements of R/I correspond to polynomials of degree less than 4. Such a polynomial has coefficients of 1, x, x^2, and x^3 which may be 0 or 1, so there are $2^4 = 16$ elements; $(R/I)^*$ has 15 elements, namely all nonzero elements of R/I. Their orders are the divisors of 15, namely $1, 3, 5, 15$. (1 mark each, total 3) [lecture and homework]

9ii. We calculate directly:

$$\begin{aligned}
(x^2+x)^1 &= x^2 + x \neq 1 \\
(x^2+x)^2 &= x^4 + x^2 \\
&= x^2 + x + 1 + x^4 + x + 1 \\
&= x^2 + x + 1 \text{ in R/I,} \\
(x^2+x)^3 &= (x^2+x)^2(x^2+x) \\
&= (x^2+x+1)(x^2+x) \\
&= x^4 + x \\
&= 1 + x^4 + x + 1 \\
&= 1 \text{ in R/I,}
\end{aligned}$$

so the order is 3. (3 marks) [lecture and homework]

9iii. We have $(x^2+x)(x^3+x) = x^5 + x^4 + x^3 + x^2 = x^4 + x^3 + x = x^3 + 1$, and $(x^2+x) + (x^3+x) = x^2 + x^3$. (3 marks each) [lecture and homework]

9iv. The order is 15. It is clearly not 1; if it were 3 then $(x^3+x)^3$ would be 1, which it is not; if it were 5 then $(x^2+x)^5$ would be 1, which it is not; so it must be 15. (3 marks) [lecture]

10ia. There are $\binom{14}{2} = 91$ subsets of order 2 in a set of order 14, and $\binom{5}{2} = 10$ in a set of order 5. For each of 91 things to appear twice in a list of lists of 10 things is impossible, because 10 does not divide $91 \cdot 2$. (It is acceptable to state the criterion as a theorem.) (5 marks) [lecture and homework]

10ib. Again, there are 105 subsets of order 2 in a set of size 15, and 15 in a set of size 6. Thus we would have to have 7 sets of size 6. But a 2-design is a 1-design, and thus we would need 15 to divide $7 \cdot 6$, which it does not. (5 marks) [lecture and homework]

10ii. This uses the standard results on difference sets: if a subset of $\mathbf{Z}/p$ of size r has each element of $\mathbf{Z}/p$ as a difference k times, then developing it gives a 2-(p, r, k)-design. In particular, we notice that the differences of the set $\{0, 1, 4, 6\}$ are $1, 4, 6, 12, 9, 7, 3, 10, 5, 8, 2, 11$. Thus all the differences occur exactly once, and therefore we get a 2-$(13, 4, 1)$-design. (5 marks) [lecture and homework]

11i. We divide $x^3 + 3x^2 + 2x + 4$ into $x^6 + 4 = x^6 - 1$. x^3 goes x^3 times into x^6, leaving $2x^5 + 3x^4 + x^3 + 4$; then x^3 goes $2x^2$ times into $2x^5$, leaving $2x^4 + 2x^3 + 2x^2 + 4$; then x^3 goes $2x$ times into $2x^4$, leaving $x^3 + 3x^2 + 2x + 4$; and x^3 goes once into x^3, leaving 0. So the quotient is $x^3 + 2x^2 + 2x + 1$. (Of course, students will generally write this as long division.) [lecture and homework] (2 marks)

11ii. The matrix is

$$\begin{pmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}.$$

(Minor variations of this are likely, e.g., the rows could be written in any order.) (4 marks) [lecture and homework]

11iii. If no column of a check matrix is 0 and no two columns are linearly dependent, then the code corrects at least one error. (3 marks) [lecture]

11iv. In each case we multiply the matrix by the given word. For 231204 we get 244, which is twice the fourth column, so we subtract 000200 to get 231004. For 111102 we get 100, the first column, so subtract 100000 to get 011102. For 121303 we get 000, so this word is in the code. (2 marks each) [lecture and homework]