Solutions for May 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) 6 is a zero-divisor in $\mathbf{Z}/8$ because $6 \cdot 4 = 0$ in $\mathbf{Z}[8]$. [lecture] (2 marks)
   (b) 4 is not a zero-divisor in $\mathbf{Z}/11$ because $\mathbf{Z}/p$ has no zero-divisors when p is prime. [lecture] (2 marks)
   (c) $3x^2 + 5x + 7/3$ is not a zero-divisor in $\mathbf{Q}[x]$ because $\mathbf{Q}$ has no zero-divisors, and we know that if R has no zero-divisors neither does $R[x]$. [similar to lecture] (2 mark)
   (d) $x-1$ is a zero-divisor in $\mathbf{Z}/2[x]/(x^5-1)$ because $(x-1)(x^4+x^3+x^2+x+1) = 0$ in $\mathbf{Z}/2[x]/(x^5-1)$. (It is acceptable to explain this by saying that $x-1$ divides x^5-1.) [similar to lecture] (2 marks)

2a. We have $d(r) = 45$, $d(s) = 50$, so let's divide s by r. This gives $s/r = (7+i)/(-3+6i) = (-15-45i)/45 = -1/3 - i$. The closest element of $\mathbf{Z}[i]$ to this is $-i$, so we have $7 + i = (-i)(-3+6i) + 1 - 2i$ and $\gcd(r, s) = \gcd(1-2i, -3+6i)$. Since $-3+6i = -3(1-2i)$, the GCD is $1-2i$. Also from the previous equation we have $7 + i + i(-3+6i) = 1 - 2i$. [similar to lecture and homework] (4 marks)

2b. Choosing to divide s by r, we get $s = 2r + 4x^2 + x + 4$, then $r = (4x+2)(4x^2+x+4) + 3$, and since 3 is a unit it is a GCD. Working backwards to find a and b, we get successively $3 = r + (x+3)(4x^2+x+4)$, then $3 = r + (x+3)(s-2r)$, and so $3 = 3xr + (x+3)s$. [similar to lecture and homework] (5 marks)

3a. It is sufficient to remove all linear factors, since $\deg f = 3$. We see that 1 is a root of f, so $x+2$ divides f, and indeed $f = (x+2)(2x^2+2)$ in $\mathbf{Z}/3[x]$. Letting $g(x) = 2x^2 + 2$, we calculate $g(0) = 2$, $g(1) = g(2) = 1$, so g has no roots and is therefore irreducible (its degree being less than 4). Thus $(x+2)(2x^2+2)$ is the factorization. [similar to lecture and homework] (3 marks)

3b. Again, it's enough to remove all linear factors, but this time one checks that $f(0) = 4, f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 3$. That is, f has no roots mod 5, so it is irreducible in $\mathbf{Z}/5[x]$. [similar to lecture and homework] (3 marks)

3c. From (b), f is irreducible in $\mathbf{Q}[x]$, so the only possible factorization is to divide through by an integer, and indeed $2|f$. So the irreducible factorization is $2(x^3 - x^2 + x + 2)$. [similar to lecture and homework] (3 marks)

4i. The required table is

$\cdot$	0	1	i	$i+1$
0	0	0	0	0
1	0	1	i	$i+1$.
i	0	i	1	$i+1$
$i+1$	0	$i+1$	$i+1$	0

(It is acceptable to choose different coset representatives.) [similar to lecture and homework] (5 marks)

4ii. A field is a ring with more than one element in which every nonzero element is a unit (or, has a multiplicative inverse, or, in which for every $r \neq 0 \in R$ there is $s \in R$ with $rs = 1$). This ring is not a field because $1+i$ is not a unit. (It is a sufficient explanation to say that $1+i$ is a zero-divisor.) [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) If $\{T_i\}$ is a 1-design, then each element of S is an element of exactly r of the T_i, so the sum of the cardinalities of the T_i is vr. On the other hand, the T_i are sets of size k and so $k|vr$. Also there are only $\binom{v-1}{k-1}$ subsets of S of size k that contain a given element (it's not necessary to explain why), so r may not be greater than this. [lecture] (6 marks)

6i. This code has dimension $5 - 3 = 2$ and its information rate is therefore $2/5$. [similar to lecture and homework] (4 marks)

6ii. To list the words, we solve the equations

$$\begin{aligned} x_1 + x_4 + x_5 &= 0 \\ x_3 + x_5 &= 0\,, \\ x_1 + x_2 + x_3 + x_5 &= 0 \end{aligned}$$

finding the general solution x_4, x_5 arbitrary, $x_3 = x_5$, $x_2 = x_4 + x_5$, $x_1 = x_4 + x_5$. Thus the codewords are 00000, 11010, 11101, 00111. From this list the minimum distance is 3 (this is the minimum number of 1's in any nonzero word) and so the code corrects $\lfloor \frac{3-1}{2} \rfloor = 1$ error. [similar to lecture and homework] (6 marks)

7. An ideal is a nonempty subset I of a ring R such if $a, b \in I$ and $r \in R$ then $a+b$ and $ar \in R$. (Minor variations of this definition are possible.) A principal ideal is an ideal consisting of the multiples of a single element of R. [lecture] (3 marks)
   a. This is an ideal. This can be seen either from the fact that it is the kernel of the homomorphism $\mathbf{Z}[x] \mapsto \mathbf{Z}/3$ given by reducing the constant coefficient mod 3, or more directly as follows: let $f = \sum a_i x^i$ and $g = \sum b_j x^j \in I$, so that $3|a_0$ and $3|b_0$. Then the constant coefficient of $f+g$ is a_0+b_0, a multiple of 3, and for any polynomial h with constant coefficient c_0 the constant coefficient of fh is a_0c_0, again a multiple of 3. [homework] (3 marks)
   b. This is not an ideal, because $3 \in I$ and $i \in R$ but $3i \notin R$. [similar to homework] (3 marks)
   c. This is not an ideal, because $4 \in I$ and $9 \in I$ but $4+9 \notin I$. [unseen] (3 marks)
   d. This is an ideal. Again this can be seen directly, by taking a_0+b_0i, a_1+b_1i in the ideal and $c+di$ in the ring and noticing that $a_0+b_0i+a_1+b_1i = (a_0+a_1)+(b_0+b_1)i$, so that $(a_0+a_1)+(b_0+b_1) = (a_0+b_0)+(a_1+b_1)$, the sum of two even numbers, is even. Then $(a_0+b_0i)(c+di) = (a_0c-b_0d)+(a_0d+b_0c)i$, and $a_0c - b_0d + a_0d + b_0c = (a_0+b_0)(c+d) - 2b_0d$ is also even. This time it is definitely easier to notice that this set is the kernel of the homomorphism $\phi : \mathbf{Z}[i] \mapsto \mathbf{Z}/2$ defined by $\phi(a+bi) = a+b \pmod 2$. [similar to lecture and homework] (3 marks)

8 A prime ideal is an ideal I of a ring R such that if $a, b \in R$ and $ab \in I$ then $a \in I$ or $b \in I$ and I is not all of R. (3 marks)

If I is prime, then I is not all of R, so R/I is nontrivial. In addition, if I is prime and $(c+I)(d+I) = 0$ for $c+I$, $d+I \neq 0 \in R/I$, then c, $d \notin I$ but $cd \in I$, contradiction. Together this proves that R/I is an integral domain. (6 marks)

If R/I is an integral domain, it is nontrivial, so I is not all of R. In addition, if $cd \in I$ for c, $d \notin I$, then $(c+I)(d+I) = 0$ in R/I but $c+I$, $d+I \neq 0$, which contradiction proves that I must be prime. (6 marks) [lecture]

Omitting the two bits on nontriviality only costs marks once.

9i. R/I has $3^3 = 27$ elements, and, because R/I is a field, all but one of those is an element of $(R/I)^*$, so there are 26. The possible orders of these elements are the divisors of 26, namely 1, 2, 13, 26. [similar to lecture and homework] (6 marks)

9ii. Indeed, $(x^2+1)^2 = x^4 + 2x^2 + 1 = xf + x + 1$ in R, so it is $x+1$ in R/I. [similar to lecture and homework] (3 marks)

9iii. Clearly the order is not 1 or 2, and $(x^2+1)^{26} = 1$ in R/I. So $(x+1)^{13} = (x^2+1)^{26} = 1$ in R/I, and the order is 13. [similar to homework] (6 marks)

10a. The lines on a projective plane over a field of 2 elements give a 2-$(7,3,1)$-design. Abbreviating the elements as 001, 010, 011, 100, 101, 110, 111, the sets are $(001, 010, 011)$, $(001, 100, 101)$, $(001, 110, 111)$, $(010, 100, 110)$, $(010, 101, 111)$, $(011, 100, 111)$, and $(011, 101, 110)$. [lecture] (8 marks)

10b. Similarly, the lines an affine plane over a field of 8 elements give a 2-$(64, 8, 1)$-design. Such a field exists because 8 is a power of 2 (more of an explanation is not necessary). (6 marks) [lecture]

5 marks for checking that these designs don't violate the numerical constraints.

11i. Indeed, the quotient is $x^3 + x + 1$. [lecture and homework] (2 marks)

11ii. The check matrix is formed by writing rows which represent the product of the quotient from (i) by powers of x, written in order of decreasing powers: thus

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

[lecture and homework] (4 marks)

11iii. The desired theorem is that no column of the check matrix should be a multiple of any other, which is easily seen to be true in this case. [lecture and homework] (3 marks)

11iv. To decode the word v, we compute Mv^t, getting respectively 01011, 00000, and 00002. Thus the first word is wrong in the place corresponding to the column that is a multiple of 01011, that is, the fourth; the word should be 21011202. The second word is correct, and the third word is wrong in the first column; it should be 20221011. [lecture and homework] (2 marks each)