Solutions for 747 exam

1. A ring homomorphism is a function $\phi : R \to S$ such that $\phi(1) = 1$ and for all $a, b \in R$ we have $\phi(ab) = \phi(a)\phi(b)$ and $\phi(a+b) = \phi(a) + \phi(b)$. (4 marks) [lecture]

1a. This is a homomorphism, because evaluation of polynomials is always a homomorphism. (4 marks) [lecture]

1b. Not a homomorphism, because (for example) $\phi((1+i)^2) = \phi(2i) = 2 \neq \phi(1+i)^2 = 2^2 = 1$. (4 marks) [lecture and homework]

1c. Not a homomorphism, because $\phi(1) \neq 1$. (4 marks) [lecture and homework]

1d. This is a homomorphism (it is the quotient map by the ideal (3)). (4 marks) [lecture and homework]

2ia. Let $g = ra + sb$. By definition of "euclidean domain", it follows that $a = qg + t$ with $t = 0$ or $d(t) < d(g)$. In the latter case we have $t = (1 - qr)a + (-s)b$, contradicting the definition of g, so t must be 0. It follows that $g|a$. (10 marks) [lecture]

2ib. We may write $a = kh$, $b = lh$. Then $g = ra + sb = rkh + slh = (rk + sl)h$. (4 marks) [lecture]

2ii. This is the GCD of a and b. To find it, we note that $N(a) > N(b)$, and then $a = -ib + (1 - i)$ and $b = (-4 + i)(1 - i)$, so the GCD is $(1 - i)$ (or any associate of this). Clearly $a + ib = 1 - i$, so we may take $r = 1$ and $b = i$. (6 marks) [lecture and homework]

3. An irreducible in an integral domain R is an element a such that a is neither 0 nor a unit, and if $a = bc$ with $b, c \in R$ then b or c is a unit. A prime in an integral domain R is an element a such that a is not a unit (optionally: also not 0), and if $a|bc$ with $b, c \in R$ then $a|b$ or $a|c$. [2 marks each, total 4] (lecture)

3a. Checking the given list, we see that $1 + i$ and $1 + 2i$ divide $-7 + 11i$. The quotient is $4 + i$, which has norm 17, so it is irreducible, and the answer is $(1 + i)(1 + 2i)(4 + i)$. [4 marks] (lecture and homework)

3b. The irreducible polynomials of degree ≤ 2 over $\mathbf{Z}/2$ are $x, x + 1, x^2 + x + 1$. None of these divides the given polynomial, so it is irreducible. [4 marks] (homework)

3c. This is irreducible, because it reduces mod 2 to the polynomial in (b) and the leading coefficient is not a multiple of 2. [4 marks] (lecture and homework)

3d. This is a multiple of 3, so we get $3(x^3 + 6x^2 - x + 4)$. The second factor reduces mod 3 to $x^3 + 2x + 1$, which has no roots and so is irreducible; thus that is the factorization. [4 marks] (lecture and homework)

In parts (a) and (d) of this problem, any factorization is acceptable; a different order or different associates of these are allowed.

4i. Clearly $\phi(1) = 1$. For the remainder, we calculate that

$$\begin{aligned}\phi(a + b\sqrt{3} + c + d\sqrt{3}) &= a + 5b + c + 5d \\ &= (a + 5b) + (c + 5d) \\ &= \phi(a + b\sqrt{3}) + \phi(c + d\sqrt{3})\end{aligned}$$

and

$$\begin{aligned}\phi((a + b\sqrt{3})(c + d\sqrt{3})) &= (a + 5b)(c + 5d) \\ &= ac + 5cb + 5ad + 3bd \\ &= \phi(ac + 3bd + (ad + bc)\sqrt{3}) \\ &= \phi(a + b\sqrt{3})\phi(c + d\sqrt{3}).\end{aligned}$$

Now, $\phi(1 + 2\sqrt{3}) = 1 + 10 = 0$ in $\mathbf{Z}/11$, so the kernel contains $(1 + 2\sqrt{3})$ because it is an ideal. (8 marks) [very similar to lecture and homework]

4ii. Indeed, $11 = (2\sqrt{3} + 1)(2\sqrt{3} - 1)$. (4 marks) [very similar to lecture and homework]

4iii. Let $a + b\sqrt{3} \in \ker \phi$, so that $11|(a + 5b)$. Then, as suggested,

$$a(1 + 2\sqrt{3}) - (2a + 10b - 11b)\sqrt{3} \in \ker \phi.$$

From the above, $a(1+2\sqrt{3})$ and $11b\sqrt{3} \in (1+2\sqrt{3})$. Also, because $11|(a+5b)$, it divides $-(2a+10b)\sqrt{3}$, and so $(1 + 2\sqrt{3})| - (2a + 10b)\sqrt{3}$, as desired. (8 marks) [very similar to lecture and homework]

5i. The desired property is that f should be irreducible. $f = x^2 + 3$ is irreducible because it has no roots: evaluating it at $x = 0, 1, 2, 3, 4$ gives $f(x) = 3, 4, 2, 2, 4$ respectively. (6 marks) [lecture and homework]

5ii. The powers of x are $x, 2, 2x, 4, 4x, 3, 3x, 1$, so the order of x is 8. The powers of $3x+2$ are $3x+2, 2x+2, 1$, so the order of $3x+2$ is 3. A generator has order 24, so an element of order n is a square if and only if $24/n$ is even. In particular, x is not a square but $3x+2$ is. (4 marks each, total 8) [lecture and homework]

5iii. $x(3x+2) = 3x^2 + 2x = 2x + 1$, because $x^2 = 2$ in R. If two elements have relatively prime order, the order of the product is the product of the orders, so the order of $2x+1$ must be 24. (6 marks) [lecture and homework]

6i. The smallest such prime is 2. The polynomial reduces mod 2 to $x^3 + x^2 + x + 1 = (x+1)^3$. (4 marks) [lecture and homework]

6ii. The smallest such prime is 5. The values of f mod 5 are $3, 2, 1, 1, 3$, so f is irreducible mod 5. Since f is an integral polynomial whose leading coefficient is not a multiple of 5, this shows that f is irreducible in $\mathbf{Q}[x]$. (4 marks) [lecture and homework]

6iii. The problem asks, in effect, for a polynomial g such that $f|(g(x^2 - x - 2) - 1)$. We start by finding the GCD of f and $x^2 - x - 2$. We have $f = (x^2 - x - 2)(x - 2) + x - 1$, and then $x^2 - x - 2 = (x-1)x - 2$, so -2 is a GCD and we can write

$$\begin{aligned} -2 &= x^2 - x - 2 - (x-1)x \\ &= (-x)(f - (x-2)(x^2 - x - 2)) + (x^2 - x - 2) \\ &= -xf + (x^2 - 2x + 1)(x^2 - x - 2). \end{aligned}$$

It follows that $(x^2 - 2x + 1)(x^2 - x - 2) = -2$ in R, so that $(x^2 - x - 2)^{-1} = (-1/2)(x^2 - 2x + 1) = -x^2/2 + x - 1/2$. (8 marks) [lecture and homework]

6iv. The above shows that $1/(\alpha^2 - \alpha - 2) = -1/2 + \alpha - \alpha^2/2$. (It is acceptable to write only $a = -1/2, b = 1, c = -1/2$.) (4 marks) [lecture]

7i. To develop a subset S of $\mathbf{Z}/n$ is to give the sets $\{a + i : a \in S\}$ for all $i \in \mathbf{Z}/n$. (4 marks) [lecture]

7ii. If n is prime and every nonzero element of $\mathbf{Z}/n$ is a difference of a pair of elements of S in the same number k of ways, then developing S creates a 2-design, then developing S gives a 2-$(n, |S|, k)$-design. (5 marks) [lecture] In particular, the differences of $\{0, 1, 4, 6\}$ are $1, 4, 6, 12, 9, 7, 3, 10, 5, 8, 2, 11$, which are all the nonzero elements of $\mathbf{Z}/13$. (2 mark) [lecture]

7iii. A 3-element set has 6 pairwise differences, so it is impossible to hit each of the 12 nonzero elements of $\mathbf{Z}/13$ the same number of times. (3 marks) [unseen]

7iv. The differences of the set $\{0, 1, 4\}$ are $1, 4, 12, 9, 3, 10$, and those of $\{0, 2, 7\}$ are $2, 7, 11, 6, 5, 8$, so between these we have every nonzero element of $\mathbf{Z}/13$ exactly once. Thus, let $\{a, b\}$ be a 2-element subset of $\mathbf{Z}/13$. If $a - b \in \{1, 4, 12, 9, 3, 10\}$, then $\{a, b\} \subset \{i, 1 + i, 4 + i\}$ for a unique i, and if $a - b \in \{2, 7, 11, 6, 5, 8\}$ then $\{a, b\} \subset \{i, 2 + i, 7 + i\}$ for a unique b. (The sufficiently patient student can do this by hand.) (5 marks) [similar to homework]

8i. The factorization is $(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$. (This factorization will be explicitly presented in lecture. Of course it can be found by trial and error.) (3 marks) [lecture]

8ii. There are two possibilities: $(x+1)(x^3+x+1) = x^4+x^3+x^2+1$, and $(x+1)(x^3+x^2+1) = x^4+x^2+x+1$. For the rest of this solution we will use the first, the situation with the second being very similar. The check matrix is

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

(Minor variations are possible and receive full credit if correct.) (5 marks) [lecture and homework]

8iii. The columns of the check matrix are all nonzero and no two are linearly dependent, so at least one error is corrected and the minimum weight is at least 3. It is at most 4, because 1110100 is a codeword. If it were 3, there would be a word of odd weight. But this is impossible, because any codeword corresponds to a multiple of $x^4 + x^3 + x^2 + 1$ in $\mathbf{Z}/2[x]/(x^7 + 1)$, so to a multiple of $x + 1$. Therefore it takes the value 0 at 1, and this cannot be changed by adding multiples of $x^7 + 1$, so it must have even weight. Thus it is 4.

Alternative argument: the generators of the code all have weight 4. Now, the weight of a sum of two words over $\mathbf{Z}/2$ is the sum of the weights less twice the number of positions where the words have the same symbol; in particular, if both words are of even weight, their sum is too, and hence this holds for all words of the given code.

Second alternative argument: the sum of rows 1, 3, 4 of the check matrix is 1111111, so the code can have no words of odd weight, because the product of 1111111 with such a word could hardly be 0.

(9 marks) [lecture and homework]

8iv. The number of errors corrected is $\lfloor (4-1)/2 \rfloor = 1$. (3 marks) [lecture and homework]