Solutions for third-year exam

1. A ring homomorphism is a function ϕ from a ring R to a ring S such that $\phi(1) = 1$ and for all r and s we have $\phi(r+s) = \phi(r) + \phi(s)$ and $\phi(rs) = \phi(r) + \phi(s)$. [lecture] (4 marks)
   (a) Not a homomorphism, because $\phi(1+1) = 4 \neq 2 = \phi(1) + \phi(1)$. [lecture] (4 marks)
   (b) This is a homomorphism whose kernel is the principal ideal $(x^2 - 2)$ and whose image is $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$. [lecture, or very similar to it] (4 marks)
   (c) Not a homomorphism, because $\phi(1) \neq 1$. [lecture] (4 marks)
   (d) Surjective homomorphism with kernel (5). [lecture] (4 marks)

2i. We must show that $0 \in (r, s)$, that if m, $n \in (r, s)$ then $m + n \in (r, s)$, and that if $m \in (r, s)$ and $t \in R$ then $mt \in (r, s)$. The first is true because $0 = 0r + 0s$. For the second, if $m = ar + bs$ and $n = cr + ds$ then $m + n = (a + c)r + (b + d)s$. For the third, if $m = ar + bs$ then $mt = (at)r + (bt)s$. [lecture] (8 marks)

2ii. Let d be a Euclidean function for R, and choose nonzero $t \in (r, s)$ such that $d(t)$ is minimal. We show that $(t) = (r, s)$: indeed, any multiple ct of t is equal to $acr + bcs$, showing that $(t) \subseteq (r, s)$. On the other hand, suppose that $ar + bs \in (r, s)$ does not belong to (t). Then we may write $ar + bs = qt + r$ where $r \neq 0$ is such that $d(r) < d(t)$, contradiction. [lecture] (8 marks)

2iii. We use the Euclidean algorithm for GCD, finding $\gcd(4 + 7i, 7 + 9i) = \gcd(3 + 2i, 4 + 7i) = 3 + 2i$ because $4 + 7i = (2 + i)(3 + 2i)$. [similar to homework] (4 marks)

3i. Clearly $\phi(1) = 1$. Taking $a + b\sqrt{2}$ and $c + d\sqrt{2}$ to be arbitrary elements of R, we find that

$$\begin{aligned}\phi(a + b\sqrt{2} + c + d\sqrt{2}) &= (a + c) + 3(b + d) \pmod 7 \\ &= a + 3b + c + 3d \pmod 7 \\ &= \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}).\end{aligned}$$

Likewise we calculate

$$\begin{aligned}\phi((a + b\sqrt{2})(c + d\sqrt{2})) &= \phi(ac + 2bd + (ad + bc)\sqrt{2}) \\ &= ac + 2bd + 3ad + 3bc \pmod 7 \\ &= ac + 9bd + 3ad + 3bc \pmod 7 . \\ &= (a + 3b)(c + 3d) \pmod 7 \\ &= \phi(a + b\sqrt{2})\phi(c + d\sqrt{2})\end{aligned}$$

Clearly $\phi(3 - \sqrt{2}) = 0 \pmod 7 = 0$, so $3 - \sqrt{2}$ is in $\ker\phi$, and therefore every multiple of $3 - \sqrt{2}$ is in the kernel. (10 marks) [similar to lecture and homework]

3ii. $(3 - \sqrt{2})(3 + \sqrt{2}) = 3^2 - (\sqrt{2})^2 = 7$. (2 marks) [similar to lecture and homework]

3iii. As suggested, let $a + b\sqrt{2} \in \ker\phi$, and let us write $a + b\sqrt{2} = (a + 3b) - b(3 - \sqrt{2})$. Now, $7|(a + 3b)$ because $a + b\sqrt{2} \in \ker\phi$, so by (ii) we get $(3 - \sqrt{2})|(a + 3b)$. Plainly $(3 - \sqrt{2})|b(3 - \sqrt{2})$, so this shows that $(3 - \sqrt{2})|(a + b\sqrt{2})$. (8 marks) [similar to lecture and homework]

4i. We have $\alpha^2 = 4 + 2\sqrt{3}$ so that $\alpha^2 - 2\alpha = 2$ and so $m_\alpha = x^2 - 2x - 2$. Similarly $\beta^2 = 1 - \frac{sqrt3}{2}$, so $\beta^2 + \beta - 1/2 = 0$ and $m_\beta = x^2 + x - 1/2$. (Any associates of these are acceptable.) [similar to lecture] (8 marks)

4ii. By direct calculation, $\alpha = 2\beta + 2$ and $\beta = \alpha/2 - 1$. Students may find this using linear algebra: if $\alpha = a + b\beta$, then equating coefficients of 1 and $\sqrt{3}$ gives $1 = a - b/2$ and $1 = b/2$, and similarly for the other one. [similar to lecture and homework] (4 marks)

4iii. Every element of $\mathbf{Q}(\alpha)$ is of the form $a + b\alpha$ for $a, b \in \mathbf{Q}$ (they need not explain why), and similarly for $\mathbf{Q}(\beta)$. Then, by the above, an element $a + b\alpha$ is equal to $a + b(2 + 2\beta) = a + 2b + 2b\beta$, so it is in $\mathbf{Q}(\beta)$, and an element $c + d\beta$ is equal to $c + d(\alpha/2 - 1) = c - d/2 + (d/2)\alpha$. [similar to lecture and homework] (8 marks)

5i. We need to find a polynomial g of degree ≤ 2 such that $g(x + 1) = 1$ in F. To do this, we use the Euclidean algorithm on $x + 1$ and $x^3 + 2x + 1$. One finds that $x^3 + 2x + 1 = (x^2 + 2x)(x + 1) + 1$, and so $1 = x^3 + 2x + 1 + (2x^2 + x)(x + 1)$. Therefore $2x^2 + x$ is the desired inverse. [similar to lecture and homework] (8 marks)

5ii. The possible orders are the divisors of $\#F - 1 = 26$, that is, 1, 2, 13, 26. [similar to lecture and homework] (4 marks)

5iii. If 2 were a square in F, its square root would be of order 4, which is not possible. [homework] (2 marks)

5iv. If, say, $2x^2 = a^2$ then $2 = (a/x)^2$, contradicting the result of (iii) above. [unseen?] (6 marks)

6a. This design exists, because 1-(v, k, r)-designs always exist when $k|vr$ and $k \leq \binom{v-1}{r-1}$. [similar to lecture and homework] (5 marks)

6b. This design exists, because of the theorem that a 2-$(v, 3, 1)$ design always exists when $v > 1$ is congruent to 1 or 3 mod 6. [lecture] (5 marks)

6c. This design does not exist. There are 105 pairs of elements in a set of 15 elements, and each 6-element subset contains 15, so the design would have 7 sets. This is not possible, because $6 \cdot 7$ is not a multiple of 15 (using the theorem that a 2-design is also a 1-design). [theorem presented in lecture, similar examples in homework] (5 marks)

6d. This is the projective plane over the field $\mathbf{Z}/5$. [lecture] (5 marks)

7i. Each point is given by four coordinates, not all 0. This gives $n^4 - 1$ choices, but sets of coordinates equivalent under scaling give the same point, so we divide by $n - 1$ (the number of nonzero elements of F) to get $n^3 + n^2 + n + 1$. [lecture] (8 marks)

7ii. Each plane is defined by a nontrivial linear equation in 4 variables, of which there are $n^4 - 1$, and two equations give the same plane if and only if they are scalings of each other. So we again get $(n^4 - 1)/(n - 1) = n^3 + n^2 + n + 1$. [lecture] (4 marks)

7iii. Let P and Q be points in $\mathbf{P}^3$. The number of linear equations that both satisfy is n^2, because the two conditions are independent by definition of points in projective space. One of these is trivial, and the remaining $n^2 - 1$ give $(n^2 - 1)/(n - 1) = n + 1$ different planes. Since there are $n^3 + n^2 + n + 1$ points in $\mathbf{P}^3(F)$ and $n^2 + n + 1$ on each plane, this is a 2-$(n^3 + n^2 + n + 1, n^2 + n + 1, n + 1)$-design. [lecture] (8 marks)

8. The weight of a word of a code is the number of nonzero symbols it contains. (2 marks)

(i) It is enough to check that if a and b have even weight so does $a + b$. To see this, note that for $a + b$ to have a 1 in a given place it is necessary and sufficient that a or b does but not both, so the weight of $a + b$ is the sum of weights of a and b minus twice the number of positions where a and b are both 1. In particular the weight of $a + b$ is even provided that the weights of a and b are. (6 marks)

Clearly the codewords of even weight in C are those that satisfy the one additional equation $\sum a_i = 0$: that is, the check matrix is obtained by adding an addition row of 1's. Thus the dimension decreases by 0 or 1; but it cannot be 0, since that would say that all words of C have even weight, and we are told that that is not the case. (6 marks) [lecture] (14 marks total for this part)

(ii) The simplest example is the code $C = \{0000, 1110, 0111, 0110\}$. The set of words whose weight is a multiple of 3 is not closed under addition, because it contains 1110 and 0111 but not 0110. [unseen] (6 marks)