Solutions for supplementary exam

1. A unit is an element r of a ring R such that there is $s \in R$ with $rs = 1$. That s is then called the multiplicative inverse. [lecture] (1 mark)
   a. Not a unit, because the only units in $R[x]$ when R is an integral domain are constant polynomials. [lecture] (2 marks)
   b. Unit, with multiplicative inverse $2x + 1$. [homework] (2 marks)
   c. Unit, with inverse 2. [similar to lecture and homework] (2 marks)
   d. Unit, with inverse 7. [similar to lecture and homework] (2 marks)

2a. We check that the values of this polynomial at 0, 1, 2 are 1, 1, 0 respectively, so $f(x)$ is a multiple of $x - 2 = x + 1$. Division gives $f(x) = (x + 1)(x^2 + 1)$, and now $x^2 + 1$ is checked to have no roots, so it is irreducible and this is the factorization. [similar to lecture and homework] (3 marks)

2b. Again we check that the values of this polynomial at $0, 1, 2, 3, 4 \in \mathbf{Z}/5$ are $1, 2, 2, 2, 3$, so there are no roots. A polynomial of degree 3 over a field with no roots is irreducible. [similar to lecture and homework] (3 marks)

2c. This polynomial is irreducible over $\mathbf{Z}/5$ and its leading coefficient is not a multiple of 5. It is therefore irreducible over $\mathbf{Z}$. [similar to lecture and homework] (3 marks)

3i. The single element sought is $\gcd(x^3 + x^2, x^4 + x^3 + x^2) = \gcd(x^3 + x^2, x^2) = x^2$. [similar to lecture and homework] (5 marks)

3ii. The sought-after multiplication table:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$.
x	0	x	0	x
$x+1$	0	$x+1$	x	1

[similar to lecture and homework] (4 marks)

4i. Let the line be $ax + by + cz = 0$. Then we have $a + 2c = 2a + b + 2c = 0$, and eliminating a from the second equation we get $b + c = 0$, that is, $a = c$ and $b = -c$. So the line is $2x + y + 2z = 0$ or $x + 2y + z = 0$ (either form is acceptable.) [similar to lecture and homework] (4 marks)

4ii. Let's take the form $x + 2y + z = 0$. With $z = 1$ we get $x + 2y = 2$, and putting successively $y = 0$, 1, 2 we get the points $[2 : 0 : 1]$, $[0 : 1 : 1]$, $[1 : 2 : 1]$. With $z = 0$ we get $x + 2y = 0$. We do not get a point with $y = 0$, and $y = 1$ give the point $[1 : 1 : 0]$—four points in all. (Other forms of the answer are acceptable.) [similar to lecture and homework] (5 marks)

5i. A t-(v, k, r)-design is a set of subsets of size k of a v-element set such that every subset of size t appears exactly r times. [lecture] (3 marks)

5ii. The sets $\{1, 2, 3, 4\}$, $\{1, 2, 5, 6\}$, $\{3, 4, 5, 6\}$ constitute such a design. (Any of the numerous correct answers is acceptable.) [similar to lecture and homework] (3 marks)

5iii. No, because $\{1, 2\}$ is a subset of two of these; $\{1, 3\}$, of only one (or as appropriate; it's also acceptable to cite the theorem that for a 2-design we need to have $r\binom{v}{2}/\binom{k}{2}$ sets). [similar to lecture and homework] (3 marks)

6i. The factorization is $(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. [lecture] (5 marks)

6ii. There is no such code, because its generator would have to be a degree-2 factor of $x^7 + 1$ over $\mathbf{Z}/2$, and the above shows that no such exists. [similar to lecture] (5 marks)

7. A subring of a ring R is a subset that contains 1 and is closed under negation, addition, and multiplication. [Minor variations are possible.] [lecture] (3 marks)
   a. Not a subring, because it doesn't contain 1. [lecture] (3 marks)
   b. Not a subring, because it isn't closed under negation. [lecture] (3 marks)
   c. Yes, this is a subring. $1 = 1 + 0\sqrt{-3} \in S$, and if $t = a + b\sqrt{-3}$ and $u = c + d\sqrt{-3}$ are in S then so are $t + u = a + c + (b + d)\sqrt{-3}$ and $tu = ac - 3bd + (ad + bc)\sqrt{-3}$. [similar to lecture] (3 marks)
   d. Yes, this is a subring. $1 \in S$, and if $f = a_0 + a_3x^3 + \ldots + a_mx^m$ and $g = b_0 + b_3x^3 + \ldots + b_nx^n$ are in S then so are
   $$f + g = (a_0 + b_0) + (a_3 + b_3)x^3 + \ldots$$

and

$$fg = (a_0b_0) + (a_0b_3 + a_3b_0)x^3 + (a_0b_4 + a_4b_0)x^4 + \ldots + a_mb_nx^{m+n}.$$

[similar to lecture] (3 marks)

8. A homomorphism of rings is a function $\phi : R \mapsto S$ from one ring to another such that $\phi(1) = \phi(1)$, $\phi(a+b) = \phi(a) + \phi(b)$, and $\phi(ab) = \phi(a)\phi(b)$. [lecture] (3 marks)
   i. That $\phi(1) = 1$ is clear (but must be stated). For the other two, let $f = \sum a_j x^j$ and $g = \sum b_k x^k$ be polynomials. Then $f(i) + g(i) = \sum a_j i^j + \sum b_k i^k = \sum (a_l + b_l) i^l = (f+g)(i)$ and $f(i)g(i) = (\sum a_j i^j)(\sum b_k i^k) = \sum\sum a_{l-m} b_m i^m = fg(i)$. [lecture] (4 marks)
   ii. By definition we would have $\psi(1) = 1$. Since $\psi(-1+1) = \psi(-1) + \psi(1)$ we get $\psi(-1) = -1$ Let $f = \psi(i)$. Then $f^2 = -1$; in particular, $f(-f) = 1$, and f is a unit. So f must be a constant polynomial. But there are no constant real polynomials with square -1. [similar to homework] (8 marks)

9i. No. If n is not a prime power, there is no field of n elements. [lecture] (3 marks)

9ii. The intended condition is that R should be a field and f an irreducible polynomial. [lecture] (4 marks) $\mathbf{Z}/3$ is a field and $x^3 + 2x + 1$ (among others) is an irreducible polynomial of degree 3 over it, so $\mathbf{Z}/5\,[x]/(x^3 + 2x + 1)$ is a field. Now, according to the division algorithm for polynomials over a field, every element of this ring is represented by a unique polynomial of degree at most 2, and there are 3 choices for the coefficients of x^2, x, and 1, making $3^3 = 27$ in all. [similar to lecture] (8 marks)

10i. The subsets $123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357$ of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ constitute a 2-$(9, 3, 1)$-design. This comes from considering lines in an affine plane over the field $\mathbf{Z}/3$. [lecture] (6 marks)

10ii. The polynomial $x^2 + x + 1$ is irreducible over $\mathbf{Z}/2$, so there is a field $\mathbf{F}_4$ of order 4. The projective plane over $\mathbf{F}_4$ has order $4^2 + 4 + 1 = 21$, and every nonzero linear equation in three variables has 16 solutions, giving $(16-1)/(4-1) = 5$ points. Every two points lie on a unique line, so the set of lines in $\mathbf{P}^2(\mathbf{F}_4)$ is a 2-$(21, 5, 1)$-design. [similar to lecture] (9 marks)

11i. If the code corrects s errors, then any two words at Hamming distance at most s from codewords are different, so the total number of words is greater than or equal to the number of codewords multiplied by the number of words at distance at most s from a given word. On the other hand, there are $\binom{n}{i}(q-1)^i$ words at distance i from a given word ($\binom{n}{i}$ ways to choose the places in which they differ and $(q-1)^i$ ways to choose the symbols in those places. So we get

$$q^k \sum_{i=0}^{s} \binom{n}{i} (q-1)^i \leq q^n,$$

and a trivial rearrangement produces the formula asserted. [lecture] (7 marks)

11ii. In particular, with $n = 9$ and $s = 1$ we get $1 + 9 \leq 2^{9-k}$, so $9 - k \geq 4$ and $k \leq 5$. [similar to homework] (3 marks)

11iii. A check matrix in which no column is a multiple of any other gives a code that corrects 1 error. In particular, we need a 9 by 4 matrix with entries in $\mathbf{Z}/2$ and all its columns nonzero and different, such as

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

(Among many other equally acceptable possibilities.) [similar to homework] (5 marks)