****The following questions are concerned with Chapter 6: Polynomials and Codes.****

78 a) Show in general (and by contradiction) that if in a ring R we have $a \neq 0, b \neq 0$, but $ab = 0$, then there is no a^{-1} or b^{-1} in R.
b) Use $R = \mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ to provide an example of this: for each (nontrivial) factor of $x^3 + x^2 + x + 1$, find all its multiples in R, to show that none of them is 1. (You are finding two rows of the multiplication table for R.)

S78 a) Suppose $a \neq 0, b \neq 0$, but $ab = 0$. If a^{-1} exists then we have $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$, which is a contradiction.
b) In R, $(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1 = 0$.

$\times$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$x+1$	$x+1$	x^2+x	x^2+1	$x+1$	0	x^2+1	x^2+x
x^2+1	x^2+1	x^2+1	0	x^2+1	0	0	x^2+1

△

79 Which elements of $\mathbb{F}_5$ are primitive? Which elements of $\mathbb{F}_7$ are primitive?

S79 In $\mathbb{F}_5$, the powers of 2 are $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 = 3$. Similarly the powers of 3 are 1, 3, 9=4, 27=2. So 2 and 3 are primitive in $\mathbb{F}_5$. But the powers of 4 are only 4 and 1, so 4 is not primitive. In $\mathbb{F}_7$ the powers of 3 are 1, 3, 2, 6, 4, 5, and the powers of 5 are 1, 5, 4, 6, 2, 3. So 3 and 5 are primitive. But the powers of 2 and 4 are all 1, 2 and 4, and the powers of 6 are only 1 and 6. △

80 Working in $\mathbb{F}_7$, express each non-zero element as a power of 3. If $a = 3^i$ then what is a^{-1}, in terms of i? Now find a primitive element of $\mathbb{F}_{11}$, and answer the corresponding question.

S80

$\mathbb{F}_7$:

i	0	1	2	3	4	5	6
3^i	1	3	2	6	4	5	1
$(3^i)^{-1}$	1	5	4	6	2	3	1

$\mathbb{F}_{11}$:

i	0	1	2	3	4	5	6	7	8	9	10
2^i	1	2	4	8	5	10	9	7	3	6	1
$(2^i)^{-1}$	1	6	3	7	9	10	5	8	4	2	1

In $\mathbb{F}_7$ we have $3^6 = 3^0 = 1$, so $a^{-1} = (3^i)^{-1} = 3^{6-i}$. Similarly, in $\mathbb{F}_{11}$, where $2^{10} = 1$, we have $(2^i)^{-1} = 2^{10-i}$. (The other primitive elements of $\mathbb{F}_{11}$ you could use are 8, 7, and 6.) △

81 In $\mathbb{F}_7$, for which $1 \leq i \leq 6$ is 3^i a primitive element? In $\mathbb{F}_{11}$, for which $1 \leq i \leq 10$ is 2^i a primitive element? Can you generalise this idea? If a is a primitive element in $\mathbb{F}_p$, for which $1 \leq i \leq p - 1$ is a^i a primitive element?

S81 In $\mathbb{F}_7$, only $3 = 3^1$ and $5 = 3^5$ are primitive elements. The other powers all share a factor with 6, so $2^3 = (3^2)^3 = 3^6 = 1$; $6^2 = (3^3)^2 = 3^6 = 1$; $4^3 = (3^4)^3 = 3^{12} = 1$. Similarly in $\mathbb{F}_{11}$, only $2 = 2^1$, $8 = 2^3$, $7 = 2^7$, and $6 = 2^9$ are primitive elements, because only 1, 3, 7 and 9 do not share a factor with 10, and 2^{10} is 1, so again the powers of other powers of 2 get back to 10 "too soon". In general, in $\mathbb{F}_p$, there are $p - 1$ non-zero elements, and since a is primitive we know that $a^{p-1} = 1$, but $a^i \neq 1$ for $1 \leq i < p - 1$. So, similarly, the element a^i a primitive if and only if i is prime to (shares no factor with) $p - 1$. △

82 In lectures we used the field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$. What happens if, instead, we divide $\mathbb{F}_2[x]$ out by other $f(x)$ of degree 3 over $\mathbb{F}_2$? By considering polynomials of smaller degree, show that x^3+x+1 and x^3+x^2+1 are irreducible, but x^3+x^2+x+1 is reducible, and show how it factors. (It follows that $\mathbb{F}_2[x]/(x^3+x^2+1)$ is also the field $\mathbb{F}_8$ (see Q83) but $\mathbb{F}_2[x]/(x^3+x^2+x+1)$ is a ring (see Q78).)

S82 Let $f(x) \in \mathbb{F}_2[x]$ be of degree 3, with non-zero constant term (otherwise x is obviously a factor). Then one factor must be $x+1$, and the other could be $x^2+1=(x+1)^2$, or x^2+x+1. So the reducible options are x^3+x^2+x+1 and x^3+1, and the irreducible ones are x^3+x+1 and x^3+x^2+1. △

83 a) Find all the powers of x in $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x^2+1)$. That is, make a table giving each x^i, $0 \le i \le 7$, in the form $a_2x^2+a_1x+a_0$.
b) Use your table to find x^4+x^5 in the form x^i, and $(x^2+x+1)(x^2+x)$ in the form $a_2x^2+a_1x+a_0$.

S83 a)

i	0	1	2	3	4	5	6	7
x^i	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x	1

b) $x^4+x^5=(x^2+x+1)+(x+1)=x^2$, and $(x^2+x+1)(x^2+x)=x^4\cdot x^6=x^{10}=x^3=x^2+1$. △

84 Consider $\mathbb{F}_3[x]/(x^2+1)$. Show that in this version of $\mathbb{F}_9$, x is not a primitive element, but $x+1$ is a primitive element. (Thus, we say that x^2+1 is not a primitive polynomial over $\mathbb{F}_3$.)

S84 First, notice that in $\mathbb{F}_3$, $x^2+1=0$ has no roots, so x^2+1 is irreducible, and so $\mathbb{F}_9=\mathbb{F}_3[x]/(x^2+1)$ is indeed a field. In this field, since we identify x^2+1 with 0, we have $x^2=-1=2$. We can therefore compute the powers of x as

i	0	1	2	3	4
x^i	1	x	2	$2x$	1

The powers of x do not include all 8 non-zero elements of $\mathbb{F}_9$, and so x is not primitive in $\mathbb{F}_3[x]/(x^2+1)$, and so (x^2+1) is not a primitive polynomial over $\mathbb{F}_3$.

If we now consider powers of $(x+1)$, we find that

$$\begin{aligned}(x+1)^2 &= x^2+2x+1=2x\\(x+1)^3 &= 2x(x+1)=2x^2+2x=2x-2=2x+1\\(x+1)^4 &= ((x+1)^2)^2=(2x)^2=4x^2=x^2=2,\end{aligned}$$

and so we can complete a table of powers of $(x+1)$ as

i	0	1	2	3	4	5	6	7	8
x^i	1	$x+1$	$2x$	$2x+1$	2	$2x+2$	x	$x+2$	1

Since this does contain include all 8 non-zero elements of $\mathbb{F}_9$, $(x+1)$ is primitive in $\mathbb{F}_3[x]/(x^2+1)$. △

85 By considering possible roots, show that x^3+2x+1 is irreducible in $\mathbb{F}_3[x]$. Use Proposition 6.9 to show that $\mathbb{F}_3[x]/(x^3+2x+1)$ is a field $\mathbb{F}_q$, and find q. By writing each x^i, $0\le i\le 13$, in the form $a_2x^2+a_1x+a_0$, show that x^3+2x+1 is a primitive polynomial over $\mathbb{F}_3$. Why do we *not* need to calculate the x^i, $14\le i\le 26$, to know this?

S85 If $f(x) = x^3 + 2x + 1$ factors in $\mathbb{F}_3[x]$, it must factor into a linear and a quadratic term. Thus it must have a root in $\mathbb{F}_3$, But we have $f(0) = 1$ $f(1) = 4 = 1$, $f(2) = 13 = 1$, so it is irreducible. We have the requirements for prop 6.3 with $p = 3, r = 3$, so $\mathbb{F}_3[x]/(x^3 + 2x + 1)$ is the field $\mathbb{F}_{27}$.

i	0	1	2	3	4	5	6
x^i	1	x	x^2	$x+2$	x^2+2x	$2x^2+x+2$	x^2+x+1

i	7	8	9	10	11	12	13
x^i	x^2+2x+2	$2x^2+2$	$x+1$	x^2+x	x^2+x+2	x^2+2	2

From now on, $x^{13+i} = 2x^i$, so we will not get to 1 until x^{26}. (You could also argue that the order of the element x must divide the order of the multiplicative group $\mathbb{F}_{27} - \{0\}$, which is 26. So if the order of x is not 2 or 13, it must be 26.) So x is primitive in this version of $\mathbb{F}_{27}$, so by definition $x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$. △

86 Let a be a primitive element in the field $\mathbb{F}_q$, where the prime power $q = p^r$.
a) For which $1 \leq i \leq q - 1$ is a^i a primitive element? (See Q81; explain if you can. For a formal proof, you need Lagrange's Theorem - the order of a subgroup divides the order of the group.)
b) Show that if *every* $a \in \mathbb{F}_q, a \neq 0, a \neq 1$ is primitive, then $p = 2$.
c) Show that the converse is not true: for some values of r, $\mathbb{F}_{2^r}$ has other non-primitive elements.
d) Show that any irreducible polynomial of degree 3 or 5 in $\mathbb{F}_2[x]$ is a primitive polynomial over $\mathbb{F}_2$.

S86 a) a^i is primitive $\Leftrightarrow$ i shares no factors with $q - 1$
$\Rightarrow$, contrapositive: If i shares a factor with $q-1$, then we have $ki = m(q-1)$, with $k < q-1, m < i$. But then $(a^i)^k = 1$, so a^i is not primitive.
$\Leftarrow$, contrapositive: The powers of a^i form a subgroup of the multiplicative group $\mathbb{F}_q - 0$. The order k of this subgroup divides $q - 1$, so there is some k which divides $q - 1$ such that $(a^i)^k = 1$, so $ki = m(q - 1)$. If a^i is not primitive, then $k < q - 1$, so i must share a factor with $q - 1$.
b) If every a^i is primitive, then by part a) every $1 < i < q - 1$ shares no factor with $q - 1$. This is true if and only if $q - 1$ is prime. If the prime $p \neq 2$, then $q = p^r$ is odd, so $q - 1$ is even, so not prime. (Strictly, $p = 3$, $r = 1$ gives $q - 1 = 2$ which is prime, so in this small case we also have every element primitive.)
c) $2^4 = 16$, $2^6 = 64$, and 15 and 63 are not prime, so $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$ have non-primitive elements.
d) An irreducible polynomial $f(x)$ is called primitive over $\mathbb{F}_p$ if, when we form the field $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$, the element x is primitive in this field. If $f(x)$ has degree 3, then $\mathbb{F}_q = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_8$. So $q - 1 = 7$, which is prime, and as in part b) every element, including x, must be primitive. Similarly if $f(x)$ has degree 5, then $\mathbb{F}_q = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_{32}$, and $q - 1 = 31$, which is also prime. △

87 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$,
a) Construct a check-matrix, and then a generator-matrix for $\text{Ham}_4(2)$.
b) Decode the received word, $y = (x, x, x + 1, 1, x)$.
c) Construct a generator-matrix and a check-matrix for the extended Hamming code $\widehat{\text{Ham}}_4(2)$.
d) Show that for $\widehat{\text{Ham}}_4(2)$, some received words do not have a unique nearest neighbour.

S87 a) In this field, we just have to remember that $x^2 = x + 1$. So $L_{(0,1)} = \{(0, 1), (0, x), (0, x + 1)\}$, $L_{(1,0)} = \{(1, 0), (x, 0), (x + 1, 0)\}$, $L_{(1,1)} = \{(1, 1), (x, x), (x + 1, x + 1)\}$, $L_{(1,x)} = \{(1, x), (x, x + 1), (x + 1, 1)\}$, $L_{(1,x+1)} = \{(1, x + 1), (x, 1), (x + 1, x)\}$.

Then one choice is $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & x & x+1 \end{pmatrix}$, and (using Proposition 4.5) $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & x & 0 & 1 & 0 \\ 1 & x+1 & 0 & 0 & 1 \end{pmatrix}$.

b) With this H, $S(y) = (x, x)$, which is x times the third column of H, so we assume the error-vector is $x\mathbf{e}_3 = (0, 0, x, 0, 0)$, and decode to $(x, x, 1, 1, x)$. But if you have a different H, you have a different (though equivalent) code, and the decoding will be different. For example, with $H' = \begin{pmatrix} 1 & 0 & x+1 & x+1 & x \\ 0 & 1 & 1 & x & x \end{pmatrix}$, the given y is actually a codeword.

c) By the definition, $\widehat{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & x & x+1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$,and by Proposition 5.9 $\widehat{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & x & 0 & 1 & 0 & x \\ 1 & x+1 & 0 & 0 & 1 & x+1 \end{pmatrix}$

d) Any Hamming code has $d = 3$, so we know that no two columns of H are dependent. But then because of their last entries 1, no three columns of $\widehat{H}$ can be dependent. Because they are of length 3, any 4 columns of $\widehat{H}$ are dependent, so for $\widehat{\mathrm{Ham}}_4(2)$, $d = 4$. (This is the same idea as for Corollary 5.8. But here the codes are not strictly binary ...) It follows (see Q16a) that for any pair of codewords $\mathbf{c}_1, \mathbf{c}_2$ with $d(\mathbf{c}_1, \mathbf{c}_2) = 4$, there is a word $\mathbf{y}$ with $d(\mathbf{c}_1, \mathbf{y}) = d(\mathbf{c}_2, \mathbf{y}) = 2$. In other words, $\widehat{\mathrm{Ham}}_4(2)$, having d even, is not perfect. △

88 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^4$ have check-matrix $H = \begin{pmatrix} 1 & x+1 & x & 1 \\ 0 & x+1 & 1 & x \end{pmatrix}$. Find $d(C)$.

S88 We can see that no column is a multiple of another (the L_v for Q87 confirm this). But the last three columns add to $\mathbf{0}$ (and in any case, $d \leq n - k + 1$), so $d(c) = 3$. △

89 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$, let $C = \langle(1, 1)\rangle \subseteq \mathbb{F}_4^2$.
a) Make a decoding array for C and use it to decode $(x, 0)$, $(1, x)$, $(x + 1, x)$, and $(0, 1)$.
b) C is transmitted over a 4-ary symmetric channel with symbol-error probability p. Find the chance that a received word is successfully decoded by your array.
c) Now make a syndrome look-up table for C, and decode the same words as in a). Does it decode them to the same codewords? If not, could you make a syndrome look-up table that *does* decode like the array?

S89 a) The code $C = \langle(1, 1)\rangle = \{(0, 0), (1, 1), (x, x), (x + 1, x + 1)\} \subseteq \mathbb{F}_4^2$, so the array could be:

$(0,0)$	$(1,1)$	(x,x)	$(x+1,x+1)$
$(0,1)$	$(1,0)$	$(x,x+1)$	$(x+1,x)$
$(x,0)$	$(x+1,1)$	$(0,x)$	$(1,x+1)$
$(x+1,0)$	$(x,1)$	$(1,x)$	$(0,x+1)$

With this array (and there are many others!) we decode $(x, 0)$ to $(0, 0)$, $(1, x)$ to (x, x), $(x + 1, x)$ to $(x + 1, x + 1)$ and $(0, 1)$ to $(0, 0)$.
b) We use Proposition 2.11; that is, we add the probabilities of the error-vectors in the first column. This gives $(1 - p)^2 + 3(1 - p)p/3$.
c) A generator matrix for C is $G = (1\ 1)$, so (by Proposition 4.5) a check matrix is also $H = (1\ 1)$, and the syndrome of a word is just the sum of its entries. So two possible syndrome look-up tables would be

Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$
0	$(0,0)$
1	$(0,1)$
x	$(x,0)$
$x+1$	$(x+1,0)$

and

Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$
0	$(0,0)$
$x+1$	$(x+1,0)$
x	$(x,0)$
1	$(1,0)$

. The first one decodes like the array above, because it tells us to subtract the same assumed error-vectors. The second does not. △

90 Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^6$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 0 & 1 & x & 0 \\ 0 & 1 & 0 & 0 & 1 & x \\ 0 & 0 & 1 & x & 0 & 1 \end{pmatrix}$.

a) Find $d(C)$.
b) How many rows would there be in a syndrome look-up table for C? To cut the table shorter, let us only include syndromes $S(\mathbf{x})$ with $w(\mathbf{x}) \leq 1$. Also, we can condense several lines into one by using $\lambda\mathbf{e}_j$ as our $\mathbf{x}$'s, where λ stands for any non-zero element of $\mathbb{F}_4$.
c) Make a shortened table like this and use it to decode (if possible) the received words $(1,1,1,1,1,1)$,
$(0,\ 0,\ 0,\ x,\ 1,\ x+1), (x,\ 1,\ 0,\ x+1,\ x,\ 1)\ (0,\ x+1,\ 0,\ x+1,\ x,\ 1), (1,\ 0,\ x,\ 1,\ 0,\ x), (1,\ x,\ 0,\ x+1,\ x,\ 1)$.
d) How many received words can we decode using this table?

S90 a) By the positions of the zeros, no column is a multiple of another, but $x \cdot$col.$1+$col.$2+$col.$5 = \mathbf{0}$, so $d(C) = 3$
b) Since $q = 4, n = 6, r = n-k = 3$, so $k = 3$, we would have $q^{n-k} = 4^{6-3} = 64$ rows.
c)

Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$	Syndrome $S(\mathbf{x})$	Error-vector $\mathbf{x}$
$(0,0,0)$	$(0,0,0,0,0,0)$		
$\lambda(1,0,0)$	$\lambda(1,0,0,0,0,0)$	$\lambda(1,0,x)$	$\lambda(0,0,0,1,0,0)$
$\lambda(0,1,0)$	$\lambda(0,1,0,0,0,0)$	$\lambda(x,1,0)$	$\lambda(0,0,0,0,1,0)$
$\lambda(0,0,1)$	$\lambda(0,0,1,0,0,0)$	$\lambda(0,x,1)$	$\lambda(0,0,0,0,0,1)$

$\mathbf{y}$	$S(\mathbf{y})$	corresponding $\mathbf{x}$	decode?
$(1,1,1,1,1,1)$	(x,x,x)	none	table fails
$(0,\ 0,\ 0,\ x,\ 1,\ x+1)$	$(0,0,0)$	$(0,0,0,0,0,0)$	$(0,\ 0,\ 0,\ x,\ 1,\ x+1)$
$(x,\ 1,\ 0,\ x+1,\ x,\ 1)$	$(x,1,0)$	$1(0,0,0,0,1,0)$	$(x,\ 1,\ 0,\ x+1,\ x+1,\ 1)$
$(0,\ x+1,\ 0,\ x+1,\ x,\ 1)$	$(0,x+1,0)$	$(x+1)(0,1,0,0,0,0)$	$(0,\ 0,\ 0,\ x+1,\ x,\ 1)$
$(1,\ 0,\ x,\ 1,\ 0,\ x)$	$(0,x+1,x)$	$x(0,0,0,0,0,1)$	$(1,\ 0,\ x,\ 1,\ 0,\ 0)$
$(1,\ x,\ 0,\ x+1,\ x,\ 1)$	$(1,x,0)$	none	table fails

d) We can decode anything in any $S(\mathbf{c},1)$ round some codeword $\mathbf{c}$, and these spheres are disjoint. There are $4^3 = 64$ codewords, and $|S(\mathbf{c},1)| = 1+6\cdot 3 = 19$. So we can decode $64 \times 19 = 1216$ words out of a possible $4^6 = 4096 = |\mathbb{F}_4^6|$. (In the "table fails" cases, we could still find a nearest neighbour - see Q69.) △

91 This question uses $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$. To help you do arithmetic in this field, first make or find the table expressing each x^i, $0 \leq i \leq 7$, in the form $a_2x^2 + a_1x + a_0$.
a) Let $C = \langle\{(x,\ x^2,\ x^2+x,\ x^2+1), (0,\ 0,\ x^2,\ x), (x+1,\ x^2+x,\ 0,\ x^2+1)\}\rangle \subseteq \mathbb{F}_8^4$. Find a generator- and a check-matrix for C, and its parameters $[n,k,d]$.
b) Use your generator-matrix to encode $(x^2,\ x^2+1)$, and to channel-decode $(x,\ x^2,\ x^2+x,\ x^2+1)$.

S91 a) In $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$, we identify the polynomial x^3+x+1 with zero, so we therefore have the identity $x^3 = x^2+1$ (since our coefficients are in $\mathbb{F}_2$). We can then calculate higher powers of

x as follows:

$$\begin{aligned}
x^3 &= x+1 \\
x^4 &= x^2+x \\
x^5 &= x^3+x^2 = x^2+x+1 \\
x^6 &= x^3+x^2+x = (x+1)+x^2+x = x^2+1 \\
x^7 &= x^3+x = 1.
\end{aligned}$$

Putting this into a table like before for easy referral:

i	0	1	2	3	4	5	6	7
x^i	1	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

Now to find a generator matrix for the code, we first need to put the elements of the spanning set as the rows of a matrix and then row-reduce to check for linear dependence.

$$\begin{pmatrix} x & x^2 & x^2+x & x^2+1 \\ 0 & 0 & x^2 & x \\ x+1 & x^2+x & 0 & x^2+1 \end{pmatrix} \xrightarrow{M_1(x^2+1)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1 \\ 0 & 0 & x^2 & x \\ x+1 & x^2+x & 0 & x^2+1 \end{pmatrix}$$
$$\xrightarrow{A_{1\,3}(x+1)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1 \\ 0 & 0 & x^2 & x \\ 0 & 0 & x^2+1 & x^2+x+1 \end{pmatrix} \xrightarrow{A_{2\,3}(x^4)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1 \\ 0 & 0 & x^2 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Since there's an all 0 row, we should now remove this, and then continue to row reduce.

$$\begin{pmatrix} 1 & x & x+1 & x^2+x+1 \\ 0 & 0 & x^2 & x \end{pmatrix} \xrightarrow{M_2(x^5)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1 \\ 0 & 0 & 1 & x^2+1 \end{pmatrix} \xrightarrow{A_{2\,1}(x+1)} \begin{pmatrix} 1 & x & 0 & x+1 \\ 0 & 0 & 1 & x^2+1 \end{pmatrix} = G.$$

G is therefore a generator matrix for C. We can now use the $G \leftrightarrow H$ algorithm to find a check matrix. The matrix G is already in RREF, with leading 1s in columns 1 and 3, so a basis for $C^\perp$ (and hence the rows of a check-matrix) is given by

$$\mathbf{v}_2 = (x,1,0,0), \quad \mathbf{v}_4 = (x+1,0,x^2+1,1),$$

and hence a check matrix for C is given by

$$H = \begin{pmatrix} x & 1 & 0 & 0 \\ x+1 & 0 & x^2+1 & 1 \end{pmatrix}.$$

By considering the generator matrix, we easily see that we have $n=4$ and $k=2$, and by considering the check-matrix, we see we have $d=2$ using Theorem 4.11 (since the final two columns are linearly dependent).

b) To encode $\mathbf{x} = (x^2, x^2+1)$, we calculate $\mathbf{c}_1 = \mathbf{x} \cdot G$,

$$\mathbf{c}_1 = (x^2, x^2+1) \begin{pmatrix} 1 & x & 0 & x+1 \\ 0 & 0 & 1 & x^2+1 \end{pmatrix} = (x^2, x+1, x^2+1, 0).$$

To channel-decode $\mathbf{c}_2 = (x, x^2, x^2+x, x^2+1)$, we need to find $\mathbf{m} = (m_1, m_2)$ such that $\mathbf{m} \cdot G = \mathbf{c}_2$. By considering the positions of the leading 1s, we see that we must have $\mathbf{m} = (x, x^2+x)$. $\triangle$

92 This question uses $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2)$. To help you do arithmetic in this field, first make or find the table expressing each x^i, $0 \le i \le 8$, in the form a_1x+a_0.
Let $C = \langle\{(0,\, x+1,\, 2x+1,\, x,\, 1), (1,\, 0,\, 0,\, 2,\, x), (2,\, 1,\, 0,\, x+2,\, x)\}\rangle \subseteq \mathbb{F}_9^5$. Find a generator- and a check-matrix for C, and its parameters $[n,k,d]$. (To find d, it may help to re-write H with entries x^i.)

S92 In lectures we made the table

i	0	1	2	3	4	5	6	7	8
x^i	1	x	$2x+1$	$2x+2$	2	$2x$	$x+2$	$x+1$	1

To find the generator-matrix we must row-reduce:

$$\begin{pmatrix}1 & 0 & 0 & 2 & x\\ 2 & 1 & 0 & x+2 & x\\ 0 & x+1 & 2x+1 & x & 1\end{pmatrix} \xrightarrow{A_{1,2}(1)} \begin{pmatrix}1 & 0 & 0 & 2 & x\\ 0 & 1 & 0 & x+1 & 2x\\ 0 & x+1 & 2x+1 & x & 1\end{pmatrix}$$

$$\xrightarrow{A_{2,3}(2x+2)} \begin{pmatrix}1 & 0 & 0 & 2 & x\\ 0 & 1 & 0 & x+1 & 2x\\ 0 & 0 & 2x+1 & 1 & 2\end{pmatrix} \xrightarrow{M_3(x+2)} \begin{pmatrix}1 & 0 & 0 & 2 & x\\ 0 & 1 & 0 & x+1 & 2x\\ 0 & 0 & 1 & x+2 & 2x+1\end{pmatrix} = G$$

So in fact the original three vectors were linearly independent, and any of these matrices is a generator -matrix for C.
Then by Proposition 4.5 $H = \begin{pmatrix}1 & 2x+2 & 2x+1 & 1 & 0\\ 2x & x & x+2 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x^3 & x^2 & 1 & 0\\ x^5 & x & x^6 & 0 & 1\end{pmatrix}$. No column of the check-matrix H is a multiple of another. (From top to bottom of columns 1, 2, 3, we multiply by x^5, x^6, x^4 respectively.) But clearly columns 4, 5 and any one other are linearly dependent (and anyway, we know $d \le 3$). So $d(C) = 3$. △

93 Prove that for $f(x)$ in $\mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$, its span $\langle f(x)\rangle$ is a cyclic code. (This is Proposition 6.14. Use Proposition 6.12 to prove it.)

S93 We must prove properties i) and ii) of Proposition 6.12. We can write $a(x), b(x) \in \langle f(x)\rangle$ as $a'(x)f(x), b'(x)f(x)$ for some $a'(x), b'(x) \in \mathbf{R}_n$ But then for i) $a(x)+b(x) = (a'(x)+b'(x))f(x) \in \langle f(x)\rangle$ and for ii) $r(x)a(x) = (r(x)a'(x))f(x) \in \langle f(x)\rangle$ as required. △

94 Let $g(x) \in \mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$ be monic, of degree r, and be a factor of x^n-1.
a) By considering the check-polynomial $h(x)$, show that any element of $C = \langle g(x)\rangle$ has degree $\ge r$.
b) Show that, with these conditions, $g(x)$ is the generator-polynomial of $\langle g(x)\rangle$.
c) Deduce that there is a 1-1 correspondence between monic factors of x^n-1 and cyclic codes in $\mathbf{R}_n$.

S94 a) Let $g(x)h(x) = x^n - 1$ in $\mathbb{F}_q^n$. Then $h(x)$ is the check-polynomial of C, and has degree $n-r=k$. Any element of C is $a(x)g(x)$ for some $a(x) \in \mathbf{R}_n$, and $a(x) = q(x)h(x)+r(x)$ for some $r(x)$ of degree $< k$. Then in $\mathbb{F}_q^n[x]$, $a(x)g(x) = g(x)[q(x)h(x)+r(x)] = q(x)g(x)h(x)+g(x)r(x) = q(x)(x^n-1)+g(x)r(x)$. This is $g(x)r(x)$ in $\mathbf{R}_n$. But since $0 \le deg(r(x)) < k$, we know $r \le deg(g(x)r(x)) < n$ in $\mathbb{F}_q^n[x]$, so there is no further reduction to be done when we go to $\mathbf{R}_n$, and indeed in $\mathbf{R}_n$, $deg(a(x)g(x)) = deg(g(x)r(x)) \ge r$ also.
b) As in the proof of Theorem 6.15 i), there cannot be two monic polynomials of least degree in C. So any other monic polynomial in C has degree $> r$. Thus $g(x)$ is the generator-polynomial of $\langle g(x)\rangle$.
c) From Proposition 6.14 we know that any code $\langle g(x)\rangle$ is a cyclic code, and from Theorem 6.15 that any cyclic code has a generator-matrix as described (correspondence is surjective). But also, if

$g_1(x)$ and $g_2(x)$ are monic factors of $x^n - 1$, and $C = \langle g_1(x)\rangle = \langle g_2(x)\rangle$, then by b) they are both the unique generator-polynomial of C, so must be the same (injectivity). △

95 Find all ternary cyclic codes of block-length 3. These can be regarded as both subrings (in fact, ideals) in the ring $\mathbf{R}_3 = \mathbb{F}_3[x]/(x^3-1)$ and subspaces of the vector space $\mathbb{F}_3^3$. So, first find the generator-polynomial of each, and then a generator-matrix for each. Two of the codes are trivial. For the two which are not trivial, find their parameters $[n,k,d]$. How are they related?

S95 Since in $\mathbb{F}_3[x]$ we have $x^3-1=(x-1)^3$, the factors of x^3-1 are: 1, $x-1=2+x$, $(x-1)^2 = 1+x+x^2$, and $(x-1)^3$. By Theorem 6.15 these generate all the codes we want in $\mathbf{R}_3$, but of course $x^3-1=0$ in $\mathbf{R}_3$. Then by Proposition 6.17 we can also write out the generator-matrices, and from these it is easy to find check-matrices and parameters.

generator-polynomial	generator-matrix	code in $\mathbb{F}_3^3$	check-matrix	(n,k,d)
1	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	all of $\mathbb{F}_3^3$	$(0\ 0\ 0)$?	$(3,3,1)$
$2+x$	$\begin{pmatrix}2&1&0\\0&2&1\end{pmatrix}$	$\{(0,0,0),\ (2,1,0),\ (0,2,1),$ $(1,2,0),\ (0,1,2),\ (2,0,1),$ $(1,0,2),\ (1,1,1),\ (2,2,2)\}$	$(1\ 1\ 1)$	$(3,2,2)$
$1+x+x^2$	$(1\ 1\ 1)$	$\{(0,0,0),(1,1,1),(2,2,2)\}$	$\begin{pmatrix}1&2&0\\0&1&2\end{pmatrix}$	$(3,1,3)$
0	$(0\ 0\ 0)$?	$\{(0,0,0)\}$	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	$(3,0,??)$

(In the table, the ?? acknowledges that the last, trivial code does not really have a minimum distance, because it only has one word. Also, ? admits that though $(0\,0\,0)$ does check or generate the code, it does not fully qualify as a check- or generator-matrix. In each case, if you think about dimensions, it should really have 0 rows and its rows should be linearly independent. The vector $(0,0,0)$ is linearly dependent all by itself.) From the matrices, it is clear that the two non-trivial codes (second and third in the table) are dual to each other (as are the two trivial codes). △

96 a) By considering possible roots, factor x^3-1 in the ring of polynomials $\mathbb{F}_7[x]$.
b) Using these factors, find all the non-trivial 7-ary cyclic codes of block-length 3. (There are six of them). Give a generator-polynomial and a generator-matrix for each.
c) Let C be the one of these codes with generator-matrix $G = \begin{pmatrix}3&1&0\\0&3&1\end{pmatrix}$. By finding x_1 and x_2 such that $x_1(3,1,0)+x_2(0,3,1)=(1,2,6)$, show that $(1,2,6)\in C$. (In effect, you are channel decoding.) In the same way, show that $(2,6,1)$ and $(6,1,2)$ (the cyclic shifts of $(1,2,6)$) are in C, but $(1,6,2)$ is not.

S96 a) In $\mathbb{F}_7$, we have that $1^3=1$, $2^3=8=1$, and $4^3=64=1$. These are therefore all roots of $x^3-1=0$, and so $(x^3-1)=(x-1)(x-2)(x-4)$.

b) Non-trivial factors $g_i(x)$ of (x^3-1) generate non-trivial cyclic codes of block length 3 in $R_3 = \mathbb{F}_7[x]/(x^3-1)$, with generator matrices G_i. Explicitly, we have the following:

- $g_1(x) = (x-1) = 6 + x$, which gives the generator matrix $G_1 = \begin{pmatrix} 6 & 1 & 0 \\ 0 & 6 & 1 \end{pmatrix}$.
- $g_2(x) = (x-2) = 5 + x$, which gives the generator matrix $G_2 = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix}$.
- $g_3(x) = (x-4) = 3 + x$, which gives the generator matrix $G_3 = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$.
- $g_4(x) = (x-1)(x-2) = 2 + 4x + x^2$, which gives the generator matrix $G_4 = \begin{pmatrix} 2 & 4 & 1 \end{pmatrix}$.
- $g_5(x) = (x-1)(x-4) = 4 + 2x + x^2$, which gives the generator matrix $G_5 = \begin{pmatrix} 4 & 2 & 1 \end{pmatrix}$.
- $g_6(x) = (x-2)(x-4) = 1 + x + x^2$, which gives the generator matrix $G_6 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

c) This is the code with generator matrix G_3 from above. Considering the positions of the zeros in G_3, we see that the first position of the word $(1,\,2,\,6)$ can only come from some multiple of the first row. We therefore need to take $x_1 = 3^{-1} = 5$. Similarly, the only contribution to the final position comes from a multiple of the second row, so we need to take $x_2 = 6$. We then have that

$$(1,\,2,\,6) = (5,\,6) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C.$$

Using the same ideas, we find that

$$(2,\,6,\,1) = (3,\,1) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C,$$
$$(6,\,1,\,2) = (2,\,2) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C.$$

If we try to use the same idea to find $(1,\,6,\,2)$ as the image of a message $(x_1,\,x_2)$, we would need to take $x_1 = 5$ and $x_2 = 2$. However, we find that

$$(5,\,2) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} = (1,\,4,\,2) \neq (1,\,6,\,2),$$

so $(1,\,6,\,2)$ is not a codeword, as it is not the image in C of any message. $\triangle$

97 Consider the code C of Q96c. Write down its generator-polynomial $g(x)$ and its check-polynomial $h(x)$. Use Proposition 6.20 to find out which of these polynomials are in C: $a(x) = 6x^2 + 2x + 1$, $b(x) = 2x^2 + 6x + 1$. Do your answers agree with Q96c?

S97 The generator matrix for C is $g(x) = x-4 = 3+x$. Thus the check-matrix is $h(x) = (x-1)(x-2) = x^2 + 4x + 2$. We now use this to "check" $a(x)$ and $b(x)$:
$a(x)h(x) = (6x^2+2x+1)(x^2+4x+2) = 6x^4+26x^3+21x^2+8x+2 = 6x+5+0+8x+2 = 0$
$b(x)h(x) = (2x^2+6x+1)(x^2+4x+2) = 2x^4+0x^3+29x^2+16x+22 = 2x+x^2+2x+2 = x^2+2x+4 \neq 0$ This agrees with Q96: $a(x) \leftrightarrow (1,2,6) \in C$; $b(x) \leftrightarrow (1,6,2) \notin C$. $\triangle$

98 In lectures, we found all the ternary cyclic codes of length 4. The codes we found (see Example 54) come in dual pairs, C and $C^\perp$. Find these pairs, and show that they are duals,
a) by considering their generator- and check-matrices, and using ideas from Chapter 4,
b) by considering their generator- and check-polynomials and using Proposition 6.22. (Remember that a polynomial can generate a code even if it is not that code's unique, official generator-polynomial.)

S98 Ternary cyclic codes of block-length 4 can be thought of as living in $R_4 = \mathbb{F}_3/(x_4 - 1)$ (where the codewords are polynomials of the form $a_0 + a_1x + a_2x^2 + a_3x^3$) *and* in $\mathbb{F}_3^4$ (where the codewords are vectors $(a_0,\, a_1,\, a_2,\, a_3)$).

a) In $\mathbb{F}_3^4$, if C is a $[4, k]$ code, then $C^\perp$ is a $[4, 4-k]$ code. So then if the dimensions match, we have that $C_j = C_i^\perp$ if and only if G_j is a check matrix for C_i, and this is the case if and only if every row of G_i is orthogonal to every row of G_j. In particular, we therefore must have that $G_i \cdot G_j$ is a matrix of all zeros, of dimensions $k \times (n-k)$.

Checking this, we see that $C_5 = C_1^\perp$, as $C_1 = \mathbb{F}_3^4$ with dimension 4, and $C_5 = \{\mathbf{0}\}$ with dimension 0. $C_7 = C_3^\perp$, both of dimension 2. $C_8 = C_2^\perp$, with $\dim C_8 = 1$ and $\dim C_2 = 3$. $C_4 = C_6^\perp$, with $\dim C_4 = 1$ and $\dim C_6 = 3$.

b) In $R_4 = \mathbb{F}_3/(x^4 - 1)$, we know from Proposition 6.22 that the reciprocal polynomial $\bar{h}(x)$, found from the check polynomial $h(x)$, generates the dual code. In particular, if we multiply $\bar{h}(x)$ by h_0^{-1}, then we get a monic polynomial which is the generator polynomial for the dual code.

C_1 has generator polynomial 1, and so check polynomial $x^4 - 1$ which is 0 in R_4. The reciprocal polynomial is therefore 0, which generates the trivial code C_5.

C_2 has generator polynomial $x + 1$, and therefore has check-polynomial $(x-1)(x^2+1) = x^3 - x^2 + x + 1$, and reciprocal polynomial $1 - x + x^2 - x^3$. This polynomial is not monic, but we can multiply by -1 to find the monic polynomial $-1 + x - x^2 + x^3$, which is the generator polynomial for the dual code. Since this is also the generator polynomial for C_8, we see that $C_2^\perp = C_8$.

C_3 has generator polynomial $x^2 + 1$ and therefore check-polynomial $(x-1)(x+1) = x^2 - 1$, and reciprocal polynomial $1 - x^2$. The generator polynomial for $C_2^\perp$ is therefore the monic polynomial $-1 + x^2$, which is the generator polynomial for C_7, and so $C_3^\perp = C_7$.

Finally, C_4 has generator polynomial $(x+1)(x^2+1)$, and therefore has check-polynomial $x - 1$, and reciprocal polynomial $1 - x$. The generator polynomial for $C_4^\perp$ is therefore the monic polynomial $-1 + x$, which is the generator polynomial for C_6, and so $C_4^\perp = C_6$. △

99 a) In $\mathbb{F}_2[x]$, $x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$. Let $g(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$, and write out the generator-matrix G_1 for the cyclic code $C_1 = \langle g(x) \rangle \subseteq \mathbf{R}_7 = \mathbb{F}_3[x]/(x^7 - 1)$.
b) Using just 3 EROs, row-reduce G_1 to standard form $(A \mid I)$. Find a check matrix H_1 for C_1, and explain why C_1 is a $\mathrm{Ham}_2(3)$ code.
c) Using Proposition 6.22 find a check-polynomial $h_1(x)$ for C_1, and a generator-polynomial $g_2(x)$ for code $C_2 = C_1^\perp$. Write out a generator-matrix G_2 for the cyclic code C_2.
d) But of course H_1 is also a generator-matrix for C_2. Use just one ERO to change G_2 to H_1.

S99 a) Using Theorem 6.15 and Proposition 6.17, since $g(x)$ is the generator polynomial for the code C_1, a generator matrix for this code is

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

b) Using 3 EROs, we have

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \xrightarrow[A_{14}(1)]{\substack{A_{24}(1) \\ A_{13}(1)}} \begin{pmatrix} 1 & 1 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & | & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & | & 0 & 0 & 0 & 1 \end{pmatrix},$$

which is in the form $(A \mid I_4)$. Using Proposition 4.5, a check-matrix for C_1 is therefore $H_1 = (I_3 \mid -A^t)$, or

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & | & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & | & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & | & 0 & 1 & 1 & 1 \end{pmatrix}.$$

This matrix has every non-zero vector of $\mathbb{F}_2^3$ appearing as one of it's columns, so it's a check-matrix for $\mathsf{Ham}_2(3)$, and hence $C_1 = \mathsf{Ham}_2(3)$.

c) By Proposition 6.22, a check-polynomial for C_1 is $h(x) = (x^4 + x^2 + x + 1)$, since we then have $x^7 - 1 = g(x)h(x)$. The reciprocal polynomial $\overline{h}(x) = 1 + x^2 + x^3 + x^4$ is then a polynomial which generates the dual code. Since this is monic, this is the generator polynomial for $C_2 = C_1^\perp$, and hence a generator matrix G_2 for C_2 is

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

d) We have

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{A_{31}(1)} \begin{pmatrix} 1 & 0 & 0 & | & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & | & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & | & 0 & 1 & 1 & 1 \end{pmatrix} = H_1,$$

so H_1 and G_2 are both check matrices for C_1, and generator matrices for $C_2 = C_1^\perp$. △

100 In $\mathbf{R}_n$, let $g(x)$ and $h(x)$ be monic, and $g(x)h(x) = x^n - 1$. Then we know by Q94b that $g(x)$ and $h(x)$ are the generator-polynomials for $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ respectively.
a) Specify polynomials which generate $C_1^\perp$ and $C_2^\perp$ respectively.
b) By considering generator-matrices for C_1 and $C_2^\perp$, show that these codes are equivalent.
(So, we might say that $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ are "almost dual" to each other.)
c) Conclude that in general, if $g(x)$ is monic and divides $x^n - 1$, then the codes $\langle g(x) \rangle$ and $\langle \overline{g}(x) \rangle$ are equivalent.

S100 a) By Proposition 6.22 $\overline{h}(x)$ generates $C_1^\perp$ and $\overline{g}(x)$ generates $C_2^\perp$.
b) Let $g(x) = g_0 + g_1 x + \cdots + g_r x^r$. Then by Proposition 6.22, the generator-matrices for $C_1 = \langle g(x) \rangle$ and $C_2^\perp = \langle \overline{g}(x) \rangle$ are, respectively,

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & & & & & \\ & g_0 & g_1 & \cdots & g_r & & & 0 & \\ & & g_0 & g_1 & \cdots & g_r & & & \\ & 0 & & \ddots & \ddots & & & \ddots & \\ & & & & g_0 & g_1 & \cdots & & g_r \end{pmatrix}, \quad G' = \begin{pmatrix} g_r & g_{r-1} & \cdots & g_0 & & & & & \\ & g_r & g_{r-1} & \cdots & g_0 & & & 0 & \\ & & g_r & g_{r-1} & \cdots & g_0 & & & \\ & 0 & & \ddots & \ddots & & & \ddots & \\ & & & & g_r & g_{r-1} & \cdots & & g_0 \end{pmatrix}.$$

By reversing the order of the rows of G, we get another generator-matrix for C_1. But by then reversing the order of the columns we get G', so by Proposition 3.7, $C_2^\perp$ is equivalent to C_1.

c) If $g(x)$ is monic and divides $x^n - 1$, then there must exist $h(x)$ as for a) and b), and the conclusion follows. $\triangle$

101 We can construct the Golay codes as cyclic codes. In $\mathbb{F}_2[x]$, $x^{23} - 1$ factors as

$$(x-1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)(x^{11}+x^9+x^7+x^6+x^5+x+1) = (x-1)g_1(x)g_2(x).$$

Use Q100 to show that $\langle g_1(x)\rangle$ and $\langle g_2(x)\rangle$, cyclic codes in $R_{23} = \mathbb{F}_2[x]/(x^{23}-1)$, are equivalent. In fact, they are both equivalent to the binary Golay code $\mathcal{G}_{23}$ of Section 5.3.

S101 $g_1(x) = 1x^{11} + 1x^{10} + 0x^9 + 0x^8 + 0x^7 + 1x^6 + 1x^5 + 1x^4 + 0x^3 + 1x^2 + 0x + 1$
$g_2(x) = 1x^{11} + 0x^{10} + 1x^9 + 0x^8 + 1x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1$
So $g_2(x) = \overline{g_1}(x)$. Since $g_1(x)$ is a monic factor of $x^{23} - 1$ it follows from Q100 that $\langle g_1(x)\rangle$ and $\langle g_2(x)\rangle$ are equivalent. $\triangle$

102 Let $\mathbf{a} = (1,0,4,7), \mathbf{b} = (1,2,3,4) \in \mathbb{F}_{11}^4$. Find the minimum distance and a basis for the Reed-Solomon code $\mathrm{RS}_3(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_{11}^4$.

S102 We use Proposition 6.24. Here $n = 4, k = 3$. So as $\mathrm{RS}_3(\mathbf{a},\mathbf{b})$ is MDS we know $d = n - k + 1 = 2$. A basis is $\{\varphi_{\mathbf{a},\mathbf{b}}(1), \varphi_{\mathbf{a},\mathbf{b}}(x), \varphi_{\mathbf{a},\mathbf{b}}(x^2)\} = \{(1,2,3,4),(1,0,1,6),(1,0,4,9)\}$. $\triangle$

103 Let $\mathbf{a} = (0,1,2,3,4), \mathbf{b} = (1,1,1,1,1) \in \mathbb{F}_7^5$. Find a generator-matrix for each code $\mathrm{RS}_k(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_7^5$, $1 \le k \le 4$. Then find a check-matrix for each code.

S103 Recall that the Reed-Solomon code is the image of the map $\varphi_{\mathbf{a},\mathbf{b}} : P_k \to \mathbb{F}_q^n$. In this case we have $q = 7$, $n = 5$ and $\varphi_{\mathbf{a},\mathbf{b}}(f(x)) = (b_1 f(a_1), b_2 f(a_2), \ldots, b_5 f(a_5))$. By Proposition 6.24, the elements $\varphi_{\mathbf{a},\mathbf{b}}(x^i)$ for $0 \le i \le k$ are a basis for $\mathrm{RS}_k(\mathbf{a},\mathbf{b})$, and hence can be taken as the rows of a generator matrix for $\mathrm{RS}_k(\mathbf{a},\mathbf{b})$.

We have

$$\begin{aligned}
\varphi_{\mathbf{a},\mathbf{b}}(1) &= (1,1,1,1,1) = \mathbf{b} \\
\varphi_{\mathbf{a},\mathbf{b}}(x) &= (f(a_1), f(a_2), f(a_3), f(a_4), f(a_5)) = (0,1,2,3,4) = \mathbf{a} \\
\varphi_{\mathbf{a},\mathbf{b}}(x^2) &= (0^2, 1^2, 2^2, 3^2, 4^2) = (0,1,4,2,2) \\
\varphi_{\mathbf{a},\mathbf{b}}(x^3) &= (0^3, 1^3, 2^3, 3^3, 4^3) = (0,1,1,6,1),
\end{aligned}$$

and so letting G_k be the generator matrix for $\mathrm{RS}_k(\mathbf{a},\mathbf{b})$, we have

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 2 \end{pmatrix} \qquad G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 2 \\ 0 & 1 & 6 & 6 & 1 \end{pmatrix}.$$

To find the check-matrices for each of these codes, we first find $\mathbf{c}$ as in Proposition 6.25, $\mathbf{c} = H_4$, the check-matrix for $\mathrm{RS}_4(\mathbf{a},\mathbf{b})$. We row reduce G_4 to

$$G_4' = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 4 \end{pmatrix},$$

which is in standard form $(I_4 \mid A)$, and hence a check-matrix for $\mathrm{RS}_4(\mathbf{a},\mathbf{b})$ is $H_4 = (-A^t \mid 1) = (1,3,6,3,1) = \mathbf{c} = \varphi_{\mathbf{a},\mathbf{c}}(1)$.

To find the remaining check-matrices, we then calculate

$$\varphi_{\mathbf{a},\mathbf{c}}(x) = (1\times 0, 3\times 1, 6\times 2, 3\times 3, 1\times 4) = (0,3,5,2,4)$$
$$\varphi_{\mathbf{a},\mathbf{c}}(x^2) = (1\times 0^2, 3\times 1^2, 6\times 2^2, 3\times 3^2, 1\times 4^2) = (0,3,3,6,2)$$
$$\varphi_{\mathbf{a},\mathbf{c}}(x^3) = (1\times 0^3, 3\times 1^3, 6\times 2^3, 3\times 3^3, 1\times 4^3) = (0,3,6,4,1),$$

and so if we let H_k be the check-matrix for $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, we have

$$H_3 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\end{pmatrix}\quad H_2 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\\0&3&3&6&2\end{pmatrix}\quad H_1 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\\0&3&3&6&2\\0&3&6&4&1\end{pmatrix}$$

as the remaining check-matrices. △

104 Let $\mathbf{a},\mathbf{b}$, and $\mathbf{b}'$ be vectors in $\mathbb{F}_q^n$. Show that if $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$ are two Reed-Solomon codes, they are (monomially) equivalent. Deduce from this and Proposition 6.25 that $[\mathsf{RS}_k(\mathbf{a},\mathbf{b})]^\perp$ and $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{b})$ are equivalent.

S104 For each $f(x)\in\mathbf{P}_k$, we get the codeword $\varphi_{\mathbf{a},\mathbf{b}}(f(x)) = (b_1 f(a_1),\ldots,b_n f(a_n))\in\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, and the codeword $\varphi_{\mathbf{a},\mathbf{b}'}(f(x)) = (b_1' f(a_1),\ldots,b_n' f(a_n))\in\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$. So to make $\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$ from $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, we only need to multiply all entries in position j by $b_j'\cdot b_j^{-1}$, for $1\le j\le n$. (We know that all $b_j\neq 0$).
By Proposition 6.25, $[\mathsf{RS}_k(\mathbf{a},\mathbf{b})]^\perp = \mathsf{RS}_{n-k}(\mathbf{a},\mathbf{c})$ for some $\mathbf{c}$. But we have just shown that $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{c})$ is (monomially) equivalent to $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{b})$. △

105 Let $\mathbf{a},\mathbf{a}'$, and $\mathbf{b}$ be vectors in $\mathbb{F}_q^n$, and $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$ be two Reed-Solomon codes. How could we pick $\mathbf{a}$ and $\mathbf{a}'$ to make the codes (monomially) equivalent?

S105 We can do this by making $\mathbf{a}'$ have the same entries as $\mathbf{a}$, but in a different order. In other words, for $1\le j\le n$, we set $a_j' = a_{\sigma(j)}$, for some permutation σ of $\{1,\ldots,n\}$. Now we can't just use σ on the entries of the codewords, because that would permute the b_j too. But we can go via $\mathsf{RS}_k(\mathbf{a}',\mathbf{1})$, where $\mathbf{1}=(1,\ldots,1)$, as follows: By Q104, we know that $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ is monomially equivalent to $\mathsf{RS}_k(\mathbf{a},\mathbf{1})$. We then apply σ to the entries of the codewords of $\mathsf{RS}_k(\mathbf{a},\mathbf{1})$, to get the equivalent code $\mathsf{RS}_k(\mathbf{a}',\mathbf{1})$, which is monomially equivalent to $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$. Since monomial equivalence is an equivalence relation (!), this chain of equivalences shows that $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$ are equivalent as required. △

106 Of course, there are Reed-Solomon codes over non-prime fields. But we have a clash of notation: in Section 6.2 we used x as an element of $\mathbb{F}_q$, and now in 6.5 it is the variable for our polynomials $f(x)\in\mathbf{P}_k$. So here is just one small, easy question: Let $\mathbf{a}=(1,x,x+1),\mathbf{b}=(1,1,1)\in\mathbb{F}_4^3$. Find a generator-matrix and then a check-matrix for $\mathsf{RS}_2(\mathbf{a},\mathbf{b})\subseteq\mathbb{F}_4^3$,

S106 By Proposition 6.24, $G = \begin{pmatrix}b_1&b_2&b_3\\b_1a_1&b_2a_2&b_3a_3\end{pmatrix} = \begin{pmatrix}1&1&1\\1&x&x^2\end{pmatrix}$. Then we row reduce this, in $\mathbb{F}_4$:
$G \xrightarrow{A_{1,2}(1)} \begin{pmatrix}1&1&1\\0&x+1&x\end{pmatrix} \xrightarrow{M_2(x)} \begin{pmatrix}1&1&1\\0&1&x^2\end{pmatrix} \xrightarrow{A_{2,1}(1)} \begin{pmatrix}1&0&x\\0&1&x^2\end{pmatrix}$, and by Proposition 4.5 $H = (x\ \ x+1\ \ 1)$. △