MATH747 January 2002. Solutions.

1(i) $\phi \neq S \subset R$ is a subring if $x, \; y \in S \; \Rightarrow \; x - y, \; xy \in S$.

[2 marks.]

$\phi \neq S \subset R$ is an ideal if $x, \; y \in S \; \Rightarrow \; x - y \in S$ and $x \in S, \; y \in R \; \Rightarrow \; xy \in S$.

[2 marks.]

(ii) a) $2x - 2y = 2(x - y) \in S$ for all $x, \; y \in R$ - that is, $2x, \; 2y \in S$.

$(2x)y = 2(xy) \in S$ for all $x, \; y \in R$- that is, $2x \in S, \; y \in R$.

So S is an deal - and hence also a subring.

[2 marks.]

(ii) b) S is not closed under subtraction, because, for any $x \in S$, $x - x = 0 \notin S$. So S is not a subring or ideal.

[2 marks.]

(ii) c)

$$S = \{2p + n\sqrt{2} : p, n \in \mathbf{Z}\} = \{\sqrt{2}(n + p\sqrt{2}) : p + n\sqrt{2} \in \mathbf{Z}[\sqrt{2}\} = \sqrt{2}\mathbf{Z}[\sqrt{2}].$$

$x, \; y \in \mathbf{Z}[\sqrt{2}] \; \Leftrightarrow \; \sqrt{2}x, \; \sqrt{2}y \in S \; \Rightarrow \; \sqrt{2}(x - y) \in S = \sqrt{2}\mathbf{Z}[\sqrt{2}]$.

$x, \; y \in \mathbf{Z}[\sqrt{2}] \; \Leftrightarrow \; \sqrt{2}x \in S, \; y \in \mathbf{Z}[\sqrt{2}] \; \Rightarrow \; \sqrt{2}xy \in S$.

So S is an ideal - and hence also a subring.

[3 marks.]

(iii) The muliplicaton table is:

.	.	S	$S+1$	$S+\sqrt{2}$	$S+1+\sqrt{2}$
.	.	.	.	.	.
S	.	S	S	S	S
$S+1$	.	S	$S+1$	$S+\sqrt{2}$	$S+1+\sqrt{2}$.
$S+\sqrt{2}$	.	S	$S+\sqrt{2}$	S	$S+\sqrt{2}$
$S+1+\sqrt{2}$	.	S	$S+1+\sqrt{2}$	$S+\sqrt{2}$	$S+1$

[5 marks] For any element $S + a$ of R/S, $(S + a) + (S + a) = S + 2a = S$, and S is the zero element. This is not true in $\mathbf{Z}_4$, where $1 + 1 = 2 \neq 0$. So the rings are not isomorphic.

[4 marks.]

$[20 = 2 + 2 + 2 + 2 + 3 + 5 + 4$ marks.]

(i) Standard theory for (i), standard homework for (ii) and (iii) - apart from the last part of (iii) which is not so standard.

2(i) $x^4 + x + 1 \neq 0$ at $x = 0, \; 1$. So there are no degree 1 factors. So the only way $x^4 + x + 1$ can be reducible in $\mathbf{Z}_2[x]$ is if $x^4 + x + 1 = (x^2 + x + 1)^2$. But $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. So $x^4 + x + 1$ is irreducible in $\mathbf{Z}_2[x]$.

[3 marks].

(ii)

$$F = \{J + a_0 + a_1x + a_2x^2 + a_3x^3 : a_i \in \mathbf{Z}_2, \; i = 0, \; 1, \; 2\}.$$

[1 mark.]

So F has $2^4 = 16$ elements.

[1 mark.]

$F^* = F \setminus \{0\}$ has $16 - 1 = 15$ elements.

[1 mark.]

(iii) The orders of the elements of F^* are the divisors of 15, that is, 1,3,5,15.

[2 marks.]

For $\alpha = J + x$, $\alpha^3 = J + x^3$, $\alpha^4 = J + x^4 = J + x + 1$, $\alpha^5 = (J + x)(J + x + 1) = J + x^2 + x$. So α does not have order 1, 3 or 5, and must have order 15.

[3 marks.]

The other elements of order 15 are α^n for n coprime to 15, that is, $n = 2$, 4, 7, 8, 11, 13, 14.

[2 marks.]

(iv) If $\beta^4 + \beta + 1 = 0$ then $\beta^4 = \beta + 1$ and $\beta^8 = \beta^5 + \beta^4$. So

$$(\beta^2)^4 + \beta^2 + 1 = \beta^8 + \beta^2 + 1 = \beta^5 + \beta^4 + \beta^2 + 1 = \beta^2 + \beta + \beta^4 + \beta^2 + 1$$

$$= \beta^4 + \beta + 1 = 0.$$

[2 marks.]

(v) $X^4(1 + X^{-3} + X^{-4}) = X^4 + X + 1$. So take $f(Y) = Y^4 + Y^3 + 1$. Then $f(\alpha^{-1}) = \alpha^4 + \alpha + 1 = 0$. $f(Y)$ is irreducible in $\mathbf{Z}_2[Y]$ by the same method as was used in (i) to show that $X^4 + X + 1$ is irreducible in $\mathbf{Z}_2[X]$. Hence f is the minimum polynomial of α^{-1}.

[2 marks.] Put $X = \alpha^5$. Then $X^3 + 1 = \alpha^{15} + 1 = \alpha^{15} - 1 = 0$. We have $X^3 + 1 = (X + 1)(X^2 + X + 1)$ in $\mathbf{Z}_2[X]$, and $\alpha^5 + 1 = \alpha^5 - 1 \neq 0$, so $(\alpha^5)^2 + \alpha^5 + 1 = 0$. Since $X^2 + X + 1$ is irreducible in $\mathbf{Z}_2[X]$, this is the minimum polynomial of α^5 in $\mathbf{Z}_2[X]$.

[3 marks.]

[$20 = 3 + 1 + 1 + 1 + 2 + 3 + 2 + 2 + 2 + 3$ marks.]

Standard homework exercises except for parts (iv) and (v), which are not quite so standard.

3(i). Label the seven varieties a, b, c, d, e, f g by the points in the projective plane $P^2(\mathbf{Z}_2)$, and the seven locations by the lines in $P^2(\mathbf{Z}_2)$. The three varieties grown in a location are the varieties corresponding to the three points on the line corresponding to the location. The incidence matrix of varieties in locations is therefore the same as the incidence matrix of points in lines, which is shown below.

[3 points.]

Each pair of varieties is grown together in exactly one location because there is exactly one line through any two points in $P^2(\mathbf{Z}_2)$: that is, the set of lines in $P^2(\mathbf{Z}_2)$ is a two-design.

[2 points.]

The incidence matrix is as shown.

.	.	$[1,0,0]$	$[0,1,0]$	$[0,0,1]$	$[1,1,0]$	$[1,0,1]$	$[0,1,1]$	$[1,1,1]$
$X=0$	.	0	1	1	0	0	1	0
$Y=0$	.	1	0	1	0	1	0	0
$Z=0$	.	1	1	0	1	0	0	0
$X+Y=0$	.	0	0	1	1	0	0	1
$Y+Z=0$	.	1	0	0	0	0	1	1
$X+Z=0$	.	0	1	0	0	1	0	1
$X+Y+Z=0$	.	0	0	0	1	1	1	0

[6 points.]

(ii) A 2-design with parameters (v,k,r) is a collection $\mathbf{B}$ of k-element subsets of a v-element set V such that every pair of elements of V is contained in exactly r of the sets in $\mathbf{B}$.

[2 points.]

(iii) The numerical conditions are $k-1 \mid (v-1)r$ and $k(k-1) \mid v(v-1)r$.

[2 points.]

When $k=3$ and $r=1$ these become $2 \mid v-1$ and $6 = 2\times 3 \mid v(v-1)$. So $6 \mid v-1$ or ($2 \mid v-1$ and $3 \mid v$). The first gives v is of the form $6n+1$, some $n \in \mathbf{Z}$. The second is equivalent to ($2 \mid v-3$ and $3 \mid v-3$), that is, $6 \mid v-3$, in which case $v = 6n+3$ for some $n \in \mathbf{Z}$.

[5 points]

[$20 = 3+2+6+2+2+5$ points.]

(i) is a standard homework exercise, (ii) is standard theory, (iii) is a bit of standard theory followed by a standard exercise.

4a)

$$x^7+1 = (x^3+x+1)(x^4+x^2+x+1)$$

in $\mathbf{Z}_2[x]$ by inspection - but it is also possible to use long division.

[2 marks.] The polynomial x^3+x+1 is irreducible because it does not vanish at 0 or 1, and hence has no degree one factors.

[1 mark]

Write $g(x) = x^3+x+1$ and $h(x) = x^4+x^2+x+1$. The generator matrix G and check matrix H - which are obtained from the coefficients of $g(x)$ and $h(x)$ respectively - are given by

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

[6 marks]

b) (i) Write $n = mp$. Then, in $\mathbf{Z}_2[x]$,

$$x^n + 1 = x^{mp}+1 = (x^m+1)(x^{m(p-1)} + \cdots + 1).$$

[1 mark.]
b)(ii) $x^{2^n-1}+1$ is the product in $\mathbf{Z}_2[x]$ of all irreducible polynomials of all degrees $m \mid n$ (in $\mathbf{Z}$) apart from the degree 1 polynomial x, each occurring exactly once.

[2 marks.]
b)(iii) $23 \times 89 = 2047$

[1 mark]
So since $2047 = 2^{11} - 1$, by (i), $(x^{23}+1) \mid (x^{2047}+1)$. Hence, by (ii) $x^{23}+1$ must be the product of the single degree 1 irreducble (apart for x) $x+1$ and two degree 11 irreducibles.

[2 marks]
b)(iv) $2 = 5^2 \bmod 23$.

[1 mark.]
Since 5 is invertible in $\mathbf{Z}_{23}$ (with inverse 14 - but 23 prime ensures invertibility) we have $2Q = \{(5n)^2 \bmod 23 : n \in \mathbf{Z}\} = Q$. So

$$\left(\sum_{i\in Q} \alpha^i\right)^2 = \sum_{i\in Q} \alpha^{2i} = \sum_{i\in 2Q} \alpha^i = \sum_{i\in Q} \alpha^i.$$

[4 marks]
$20 = 3+6+1+2+1+2+1+4$ marks.]
a) is a standard homework exercise. b) is mostly theory from lectures, although some parts are routine calculation.

5(i) *Kirkman's Schoolgirls Problem.* 15 girls go out walking 7 days in a row. They walk in threes. The problem is to arrange them in groups of three (on seven successive days) so that every pair of girls is in the same group of three exactly once.

[3 marks.]
Given sets

$$X_i = \{\mathbf{x_i}, \mathbf{y_i}, \mathbf{z_i}\} \subset \mathbf{Z}_2^4 \setminus \{\mathbf{0}\} \text{ for } 1 \le i \le 35,$$

where

$$\mathbf{z_i} = \mathbf{x_i} + \mathbf{y_i},$$

adding $\mathbf{x_i}$ to both sides gives $\mathbf{x_i}+\mathbf{z_i} = \mathbf{y_i}$ and adding $\mathbf{y_i}$ to both sides gives $\mathbf{y_i}+\mathbf{z_i} = \mathbf{x_i}$. Thus if X_i and X_j have two elements in common, they coincide, and $i = j$. So if X_{i+2n} are disjoint sets for $1 \le i \le 5$, for each $0 \le n \le 7$, then we can take the girls to correspond to the 15 points in $\mathbf{Z}_2^4 \setminus \{\mathbf{0}\}$, and take the groups X_{i+5n} on Day $n+1$ - and a pair of girls walk together only if they are in the same set X_i, which happens at most once - and exacly once since the number of 3-element sets in a 15 element set is

$$\binom{15}{3} = \frac{15 \times 14}{3 \times 2} = 35.$$

[5 marks]
(ii) The matrix A has 15 columns and 35 rows - since there are 7 days and 5 groups of three on each day.

[2 marks.]

Because A is the incidence matrix of a 2-design with parameters $(15, 3, 1)$, no two rows have more than one girl in common. So for any two rows of A there is at most one column in which both rows have a 1 (and this does happen). So the minimum distance between any two rows of A is 4.

[2 marks]

Similarly for any two rows of A'. there is at most one column in which both rows have a 0 (and this does happen) So the minimum distance between any two rows of A' is 4.

[1 mark]

Any row of A has exactly 3 1's and any row of A' has exactly 12 1's. So the minimum distance between any row of A and any row of A' is ≥ 9. So the code of all rows has minimum distance 4.

[2 marks]

(iii) Any column of A has 7 1's. If 2 columns have 1 in rows R_1 and R_2 (correspnding to girls) then this pair of girls are together in two different rows, which is impossible. So there is at most one row in which both columns have a 1 (and this does happen). So the minimum distance between columns of A is 12.

[2 marks]

Similarly the minimum distance between any two columns of A' is 12

[1 mark]

Any column of A has 7 1's and any column of A' has $35 - 7 = 28$ 1's. So the minimum distance between any column of A and any column of A' is $\geq 28 - 7 = 21$. So the code of all columns has minimum distance 12.

[2 marks.]

[$20 = 3 + 5 + 2 + 2 + 1 + 2 + 2 + 1 + 2$ marks.]

(i) is standard theory and (ii) and (iii) are standard homework exercises.

6. If $\alpha = \sqrt{3}$ then $\alpha^2 = 3$ and so α is a zero over $x^2 - 3$, which is irreducible over $\mathbf{Q}$ since the zeros $\pm\alpha$ are not rational: equivalently, it is irreducible in $\mathbf{Z}[x]$ since there are no integer zeros, and hence general theory implies it is irreducible in $\mathbf{Q}[x]$.

[2 marks]

Now let $\beta = \sqrt{3} + \sqrt{5}$; Then $\beta^2 = 8 + 2\sqrt{15}$ and

$$(\beta^2 - 8)^2 = \beta^4 - 16\beta^2 + 64 = 60.$$

So β is a zero of $f(x) = x^4 - 16x^2 + 4$.

[3 marks]

To show f is irreducible in $\mathbf{Q}[x]$ we only need to show it is irreducible in $\mathbf{Z}[x]$ (by standard theory). So it has a factorization in $\mathbf{Z}[x]$ of one of the following forms (since the coefficient of x^4 is 1):

$$(x + a)(x^3 + bx^2 + cx + d), \quad (1)$$

$$(x^2 + ax + b)(x^2 + cx + d). \quad (2)$$

[1 mark]

In the first case, $ad = 4$, so $a = \pm 1$, ± 2 or ± 4. But $f(\pm 1) = 11$, $f(\pm 2) = -44$, $f(\pm 4) = 4$, so none of these is possible.

[2 marks]

So it remains to consider a factorization of type (2). Since f has zero x^3 term, we must have $c=-a$. Then f has zero x term. So $ad=-bc$. So either $a=c=0$ or $b=d=\pm 2$, since $bd=4$.

Case $a=c=0$. From the coefficient of x^2 we have $b+d=-16$, while $bd=4$ gives $|b+d|\leq 5$. So this is impossible.

Case $b=d=2$. The coefficient of x^2 is $b+d-a^2=4-a^2=-16$, giving $a^2=20$, which is impossible for $a\in\mathbf{Z}$.

Case $b=d=-2$. We get $a^2=12$, which is again impossible for $a\in\mathbf{Z}$. So f is irreducible.

[6 marks: of course, there are many different ways of achieving this result.]

Note that

$$\sqrt{15}=\tfrac{1}{2}\beta^2-4\in\mathbf{Q}[\beta].$$

Hence also

$$\beta(\tfrac{1}{2}\beta^2-4)=\sqrt{15}\beta=3\sqrt{5}+5\sqrt{3}\in\mathbf{Q}[\beta],$$

and hence

$$\sqrt{3}=\tfrac{1}{2}(5(\sqrt{3}+\sqrt{5})-(3\sqrt{3}+5\sqrt{5}))=\tfrac{1}{2}(5\beta-\beta(\tfrac{1}{2}\beta^2-4))\in\mathbf{Q}[\beta].$$

[4 marks.]

So $[\mathbf{Q}[\alpha]:\mathbf{Q}]=2$ and $[\mathbf{Q}[\beta]:\mathbf{Q}]=4$. Since $\mathbf{Q}[\alpha]\subset\mathbf{Q}[\beta]$ we have

$$[\mathbf{Q}[\beta]:\mathbf{Q}]=[\mathbf{Q}[\beta]:\mathbf{Q}[\alpha]]\times[\mathbf{Q}[\alpha]:\mathbf{Q}],$$

we have $[\mathbf{Q}[\beta]:\mathbf{Q}[\alpha]]=4/2=2$.

[2 marks]

[$20=2+3+1+2+6+4+2$ marks.]

Standard homework exercise.

7(i) The number of points in $\mathbf{Z}_3^3$ is $3^3=27$.

[1 mark.]

The number of points on a line is the number of $t\in\mathbf{Z}_3$, that is, 3.

[1 mark]

(ii) We have

$$\ell(\mathbf{v_0},\mathbf{v_1})=\ell(\mathbf{v_0'},\mathbf{v_1'})\tag{1}$$

implies

$$\mathbf{v_0'}=\mathbf{v_0}+t_0\mathbf{v_1}\in\ell(\mathbf{v_0},\mathbf{v_1}),\ \mathbf{v_0'}+\mathbf{v_1'}=\mathbf{v_0}+t_1\mathbf{v_1}$$

for some $t_0\neq t_1\in\mathbf{Z}_3$, which implies that

$$\mathbf{v_0'}=\mathbf{v_0}+t_0\mathbf{v_1},\ \mathbf{v_1'}=s_0\mathbf{v_1}\text{ for some }s_0\neq 0.\tag{2}$$

In turn this implies that

$$\mathbf{v_0'}+t\mathbf{v_1'}=\mathbf{v_0}+(ts_0+t_0)\mathbf{v_1}\in\ell(\mathbf{v_0},\mathbf{v_1})$$

for all $t\in\mathbf{Z}_3$, which implies

$$\ell(\mathbf{v_0'},\mathbf{v_1'})\subset\ell(\mathbf{v_0},\mathbf{v_1})$$

and hence the two are equal, since they have the same number of points. So

$$(1) \Rightarrow (2) \Rightarrow (1)$$

and we have $(1) \Leftrightarrow (2)$.

[6 marks.]

So the number of $(\mathbf{v}_0', \mathbf{v}_1')$ with $\ell(\mathbf{v}_0', \mathbf{v}_1') = \ell(\mathbf{v}_0, \mathbf{v}_1) = \ell$ is the number of of points in ℓ times the number of nonzero elements of $\mathbf{Z}_3$, that is, $2 \times 3 = 6$. The total number of $(\mathbf{v}_0, \mathbf{v}_1)$ is therefore $27 \times (27 - 1) = 27 \times 26$. So the number of lines is

$$\frac{27 \times 26}{2 \times 3} = 9 \times 13 = 117.$$

[3 marks]

A line through $\mathbf{x}$ is of the form $\ell(\mathbf{x}, \mathbf{v})$, so is the number of nonzero $\mathbf{v}$ up to scale, since $\ell(\mathbf{x}, \mathbf{v}) = \ell)\mathbf{x}, 2\mathbf{v})$. So this is the total number of $\mathbf{v}$ divided by 2, that is, $26/2 = 13$

[2 marks.]

(iii) Clearly $\ell((a_1, b_1, c_1), (a_2 - a_1, b_2 - b_1, c_2 - c_1))$ contains (a_1, b_1, c_1) and (a_2, b_2, c_2) and by (ii) any line through (a_1, b_1, c_1) and (a_2, b_2, c_2) is $\ell((a_1, b_1, c_1), \mathbf{v})$ for some $\mathbf{v} \neq \mathbf{0}$, which means that

$$(a_2, b_2, c_2) = (a_1, b_1, c_1) + t\mathbf{v}$$

for $t = 1$ or 2. Hence $\mathbf{v}$ is a nonzero multiple of $(a_2 - a_1, b_2 - b_1, c_2 - c_1)$, and there is exactly one such line.

[4 marks]

By (i), the number of lines through any point is 13. So the set of lines in $\mathbf{Z}_3^3$ is a 1-design with parameters $(27, 3, 13)$ and a two design with parameters $(27, 3, 1)$.

[3 marks.]

$20 = 1 + 1 + 6 + 3 + 2 + 4 + 3$ marks.]

This is similar to a homework exercise, in which students were allowed to assume some facts: the first part of (ii) and the first part of (iii).

8a) The minimum distance of a code C in $\mathbf{Z}_2^n$ is

$$\min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y},\ \mathbf{x},\ \mathbf{y} \in C\},$$

where, if $\mathbf{x} = (x_1, \cdots x_n)$ and $\mathbf{y} = (y_1, \cdots y_n)$,

$$d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}.$$

[3 marks]

We define the *weight* $w(\mathbf{x})$ of $\mathbf{x} \in \mathbf{Z}_2^n$ by

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) = \#\{i : x_i \neq 0\},$$

if $\mathbf{x} = (x_1, \cdots x_n)$. Then the weight of C is

$$\min\{w(\mathbf{x}) : \mathbf{x} \in C\}.$$

[2 marks]

So

$$w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x} - \mathbf{y}) = d(\mathbf{x}, \mathbf{y})$$

If C is a linear code, then $\mathbf{0} \in C$ and $\mathbf{x}+\mathbf{y} \in C$ whenever $\mathbf{x}$, $\mathbf{y} \in C$. So for a linear code, weight and minimum distance coincide.

[3 marks]

b)(i) Let $\mathbf{x}$ have weight 1, and let the i'th entry be the only nonzero one. Writing $\mathbf{x}$ as a column vector, $H\mathbf{x}$ is the i'th column of H. This is nonzero. So $\mathbf{x}$ cannot be in C.

[2 marks.]

(ii) Let $\mathbf{x}$ have weight 2 and let the i'th and j'th entries be the nonzero ones. Then $H\mathbf{x}$ is the sum- equivalently the difference - of the i'th and j'th columns of H. These columns are distinct and therefore the difference is nonzero. So, again, $\mathbf{x}$ cannot be in C.

[2 marks]

(iii) Let $\mathbf{x}$ have weight 3 and let the i'th, j'th and k'th entries be the nonzero ones. Then $H\mathbf{x}$ is the sum of the i'th, j'th and k'th columns of H. This is nonzero. So, again, $\mathbf{x}$ cannot be in C.

[2 marks]

(iv) To show that C has weight 4, note that (11101000) is in C and has weight 4. We need to show that the sum of any 3 columns is not identically 0. The sum of any two of the last four columns, any two of the first four columns, has exactly two 1's. Hence the sum of any three of the last four columns, or any three of the first four columns is nonzero, as is the sum of any 2 of the last four with any one of the first four, or vice versa.

[6 marks.]

[$20 = 3+2+3+2+2+2+6$ marks.]

Standard theory (from lectures), except that b)(iv) is unseen.