A Book of Abstract Algebra: Chapter 3

Daniel Hughes

A. Examples of Abelian groups

Prove that each of the following sets, with the indicated operation is, an abelian group.

1. $x * y = x + y + k$ (k is fixed constant), on the set $\mathbb{R}$ of real numbers.

Proof: The operation on the set is commutative:

$$x * y = x + y + k$$

$$y * x = y + x + k$$

The operation on the set is associative:

$$\begin{aligned}(x * y) * z &= (x + y + k) * z \\ &= x + y + k + z + k \\ &= x + y + z + 2k\end{aligned}$$

$$\begin{aligned}x * (y * z) &= x * (y + z + k) \\ &= x + y + z + k + k \\ &= x + y + z + 2K\end{aligned}$$

The set contains an identity element:

$$x * e = x;\ x + e + k = x \Rightarrow e = -k$$

$$e * x = x;\ e + x + k = x \Rightarrow e = -k$$

Every element in the set has an inverse:

$$\begin{aligned}x * x^{-1} = e;\ x * x^{-1} &= -k \\ x + x^{-1} + k &= -k \\ x + x^{-1} &= -2k \\ x^{-1} &= -2k - x\end{aligned}$$

$$\begin{aligned} x^{-1} * x = e;\ x^{-1} * x &= -k \\ x^{-1} + x + k &= -k \\ x^{-1} + x &= -2k \\ x^{-1} &= -2k - x \end{aligned}$$

Therefore the operation $*$ on the set $\mathbb{R}$ forms an abelian group. ■

2. $x * y = \frac{xy}{2}$, on the set $\{x \in \mathbb{R} : x \neq 0\}$.

Proof: The operation on the set is commutative:

$$x * y = \frac{xy}{2};\ y * x = \frac{yx}{2}$$

The operation on the set is associative:

$$\begin{aligned} (x * y) * z &= \frac{xy}{2} * z \\ &= \frac{\frac{xy}{2}z}{2} = \frac{xyz}{4} \end{aligned}$$

$$\begin{aligned} x * (y * z) &= x * \frac{yz}{2} \\ &= \frac{x\frac{yz}{2}}{2} = \frac{xyz}{4} \end{aligned}$$

The set contains an identity element:

$$\begin{aligned} x * e = x;\ \frac{xe}{2} &= x \\ xe &= 2x \\ e &= 2 \end{aligned}$$

$$\begin{aligned} e * x = x;\ \frac{ex}{2} &= x \\ e &= 2 \end{aligned}$$

Every element in the set has an inverse:

$$x * x^{-1} = e \ \Rightarrow \frac{xx^{-1}}{2} = 2 \ \Rightarrow x^{-1} = \frac{4}{x}$$

$$x^{-1} * x = e \ \Rightarrow \frac{x^{-1}x}{2} = 2 \ \Rightarrow x^{-1} = \frac{4}{x}$$

Therefore the operation * on the set $\{x \in \mathbb{R} : x \neq 0\}$ forms an abelian group. ■

3. $x * y = x + y + xy$, on the set $\{x \in \mathbb{R} : x \neq -1\}$.

Proof: The operation is commutative:

$$x * y = x + y + xy; \; y * x = y + x + yx$$

The operation is associative:

$$\begin{aligned}(x * y) * z &= (x + y + xy) * z \\ &= (x + y + xy) + z + (x + y + xy)z \\ &= x + y + z + xy + xz + yz + xyz\end{aligned}$$

$$\begin{aligned}x * (y * z) &= x * (y + z + yz) \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + xy + xz + yz + xyz\end{aligned}$$

The set contains an identity element:

$$\begin{aligned}x * e = x; \; x + e + xe &= x \\ e + xe &= 0 \\ e(1 + x) &= 0 \\ e &= 0\end{aligned}$$

$$\begin{aligned}e * x = x; \; e + x + ex &= x \\ e + ex &= 0 \\ e(1 + x) &= 0 \\ e &= 0\end{aligned}$$

Every element in the set has an inverse:

$$\begin{aligned}x * x^{-1} = e; \; x + x^{-1} + xx^{-1} &= 0 \\ x^{-1}(1 + x) &= -x \\ x^{-1} &= \frac{-x}{1 + x}\end{aligned}$$

$$\begin{aligned}x^{-1} * x = e; \; x^{-1} + x + x^{-1}x &= 0 \\ x^{-1}(1 + x) &= -x \\ x^{-1} &= \frac{-x}{1 + x}\end{aligned}$$

Therefore the operation $*$ on the set $\{x \in \mathbb{R} : x \neq -1\}$ forms an abelian group. ■

4. $x * y = \dfrac{x+y}{xy+1}$, on the set $\{x \in \mathbb{R} : -1 < x < 1\}$.

Proof: The operation is commutative:

$$x * y = \frac{x+y}{xy+1};\ y * x = \frac{y+x}{yx+1}$$

The operation is associative:

$$\begin{aligned}
(x * y) * z = \frac{x+y}{xy+1} * z &= \frac{\frac{x+y}{xy+1} + z}{(\frac{x+y}{xy+1})z + 1} \\
&= \frac{\left(\dfrac{x+y+z(xy+1)}{xy+1}\right)}{\left(\dfrac{zx+zy+xy+1}{xy+1}\right)} \\
&= \frac{x+y+z+xyz}{xy+xz+yz+1}
\end{aligned}$$

$$\begin{aligned}
x * (y * z) = x * \frac{y+z}{yz+1} &= \frac{x + \frac{y+z}{yz+1}}{\frac{x(y+z)}{yz+1} + 1} \\
&= \frac{\left(\dfrac{xyz+x+y+z}{yz+1}\right)}{\left(\dfrac{xy+xz+yz+1}{yz+1}\right)} \\
&= \frac{x+y+z+xyz}{xy+xz+yz+1}
\end{aligned}$$

The set contains an identity element:

$$\begin{aligned}
x * e = x \ \Rightarrow \frac{x+e}{xe+1} = x \ \Rightarrow\ & x + e = x(xe+1) \\
& x + e = x^2e + x \\
& e(x^2 - 1) = 0 \\
& e = 0
\end{aligned}$$

$$\begin{aligned}
e * x = x \ \Rightarrow \frac{e+x}{ex+1} = x \ \Rightarrow\ & e + x = x^2e + x \\
& x + e = x^2e + x \\
& e(x^2 - 1) = 0 \\
& e = 0
\end{aligned}$$

Every element in the set has an inverse:

$$x * x^{-1} = e \ \Rightarrow \frac{x + x^{-1}}{xx^{-1} + 1} = 0 \ \Rightarrow x^{-1} = -x$$

$$x^{-1} * x = e \ \Rightarrow \frac{x^{-1} + x}{x^{-1}x + 1} = 0 \ \Rightarrow x^{-1} = -x$$

Therefore the operation $*$ on the set $\{x \in \mathbb{R} : -1 < x < 1\}$ forms an abelian group. ■

B. Groups on the Set $\mathbb{R} \times \mathbb{R}$

Which of the following subsets of $\mathbb{R} \times \mathbb{R}$, with the indicated operation, is a group? Which is an abelien group?

1. $(a, b) * (c, d) = (ad + bc, bd)$, on the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : y \neq 0\}$.

Solution. The operation on the set is associative:

$$\big((a, b) * (c, d)\big) * (e, f) = (ad + bc, bd) * (e, f) = (adf + bef + bde, bdf)$$

$$(a, b) * \big((c, d) * (e, f)\big) = (a, b) * (cf + de, df) = (adf + bef + bde, bdf)$$

The set contains an identity element:

$$\begin{aligned}(a, b) * (e_1, e_2) = (a, b);\ &(ae_2 + be_1, be_2) = (a, b)\\ &\Rightarrow be_2 = b \ \Rightarrow e_2 = 1\\ &\Rightarrow ae_2 + be_1 = a \ \Rightarrow a + be_1 = a \ \Rightarrow e_1 = 0\end{aligned}$$

$$\begin{aligned}(e_1, e_2) * (a, b) = (a, b);\ &(ae_2 + be_1, be_2) = (a, b)\\ &\Rightarrow be_2 = b \ \Rightarrow e_2 = 1,\\ &\Rightarrow ae_2 + be_1 = a \ \Rightarrow a + be_1 = a \ \Rightarrow e_1 = 0\end{aligned}$$

Therefore $(e_1, e_2) = (0, 1)$.

Every element in the set has an inverse:

$$\begin{aligned}(a, b) * (a^{-1}, b^{-1}) = (e_1, e_2) \ &\Rightarrow (ab^{-1} + ba^{-1}, bb^{-1}) = (0, 1)\\ &\Rightarrow bb^{-1} = 1 \ \Rightarrow b^{-1} = \frac{1}{b},\\ ab^{-1} + ba^{-1} = 0 \ &\Rightarrow \frac{a}{b} + ba^{-1} = 0 \Rightarrow a^{-1} = -\frac{a}{b^2}\end{aligned}$$

$$\begin{aligned}(a^{-1},b^{-1})*(a,b)=(e_1,e_2)\ &\Rightarrow (a^{-1}b+b^{-1}a,b^{-1}b)=(0,1)\\ &\Rightarrow bb^{-1}=1\ \Rightarrow b^{-1}=\frac{1}{b},\\ &ab^{-1}+ba^{-1}=0\ \Rightarrow \frac{a}{b}+ba^{-1}=0\Rightarrow a^{-1}=-\frac{a}{b^2}\end{aligned}$$

Thus $(a^{-1},b^{-1})=(-\frac{a}{b^2},\frac{1}{b})$

Therefore $(a,b)*(c,d)=(ad+bc,bd)$, on the set $\{(x,y)\in\mathbb{R}\times\mathbb{R}:y\neq 0\}$ forms a group.
It is also an abelian group as it is commutative:

$$(a,b)*(c,d)=(ad+bc,bd),\ (c,d)*(a,b)=(cb+da,db)$$

2. $(a,b)*(c,d)=(ac,bc+d)$, on the set $\{(x,y)\in\mathbb{R}\times\mathbb{R}:x\neq 0\}$.

Solution. The operation on the set is associative:

$$\big((a,b)*(c,d)\big)*(e,f)=(ac,bc+d)*(e,f)=(ace,bce+de+f)$$

$$(a,b)*\big((c,d)*(e,f)\big)=(a,b)*(ce,de+f)=(ace,bce+de+f)$$

The set contains an identity element:

$$\begin{aligned}(a,b)*(e_1,e_2)=(a,b);\ (ae_1,be_1+e_2)&=(a,b)\\ &\Rightarrow ae_1=a\ \Rightarrow e_1=1,\\ &\Rightarrow be_1+e_2=b\ \Rightarrow e_2=0\end{aligned}$$

$$\begin{aligned}(e_1,e_2)*(a,b)=(a,b);\ (e_1a,e_2a+b)&=(a,b)\\ &\Rightarrow e_1a=a\ \Rightarrow e_1=1,\\ &\Rightarrow e_2a+b=b\ \Rightarrow e_2a=0\ \Rightarrow e_2=0\end{aligned}$$

Therefore $(e_1,e_2)=(1,0)$.

Every element in the set contains an inverse:

$$\begin{aligned}(a,b)*(a^{-1},b^{-1})=(e_1,e_2);\ (aa^{-1},ba^{-1}+b^{-1})&=(1,0)\\ &\Rightarrow aa^{-1}=1\ \Rightarrow a^{-1}=\frac{1}{a},\\ &ba^{-1}+b^{-1}=e_2\ \Rightarrow \frac{b}{a}+b^{-1}=0\ \Rightarrow b^{-1}=-\frac{b}{a}\end{aligned}$$

$$\begin{aligned}(a^{-1},b^{-1})*(a,b)=(e_1,e_2);\ (a^{-1}a,b^{-1}a,+b)&=(1,0)\\ &\Rightarrow a^{-1}a=1\ \Rightarrow a^{-1}=\frac{1}{a},\\ &\Rightarrow b^{-1}a+b=0\ \Rightarrow b^{-1}=-\frac{b}{a}\end{aligned}$$

Thus $(a^{-1}, b^{-1}) = (\frac{1}{a}, -\frac{b}{a})$.

Therefore $(a, b) * (c, d) = (ac, bc + d)$, on the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x \neq 0\}$ forms a group. It is however not an abelian group because it fails commutativity.

$$(a, b) * (c, d) = (ac, bc + d) \neq (c, d) * (a, b) = (ac, da + b)$$

3. Same operation as in part 2, but on the set $\mathbb{R} \times \mathbb{R}$.

Solution. This does not form a group because not every element has an inverse. For example $(0, 5) \in \mathbb{R} \times \mathbb{R}$, but $(0, 5)^{-1} = (0^{-1}, 5^{-1}) \notin \mathbb{R} \times \mathbb{R}$ as that would result in a division by zero.

4. $(a, b) * (c, d) = (ac - bd, ad + bc)$, on the set $\mathbb{R} \times \mathbb{R}$ with the origin deleted.

Solution. The operation on the set is associative:

$$\big((a,b)*(c,d)\big)*(e,f) = (ac-bd, ad+bc)*(e,f) = (ace-bde-adf-bcf, acf-bdf+ade+bce)$$

$$(a,b)*\big((c,d)*(e,f)\big) = (a,b)*(ce-df, cf+de) = (ace-adf-bcf-bde, acf+ade+bce-bdf)$$

The set contains an identity element:

$$(a, b) * (e_1, e_2) = (a, b) \ \Rightarrow (ae_1 - be_2, ae_2 + be_1) = (a, b)$$

This gives us, the following two equations:

$$ae_1 - be_2 = a$$
$$ae_2 + be_1 = b$$

Solving yields $(e_1, e_2) = (1, 0)$.

$$(e_1, e_2) * (a, b) = (a, b) \ \Rightarrow (e_1a - e_2b, e_1b + e_2a) = (a, b)$$

This gives us, the following two equations:

$$e1_a - e_2b = a$$
$$e_1b + e_2a = b$$

Solving also yields $(e_1, e_2) = (1, 0)$.

Every element in the set contains an inverse:

$$(a, b) * (a^{-1}, b^{-1}) = (e_1, e_2) \ \Rightarrow (aa^{-1} - bb^{-1}, ab^{-1} + ba^{-1}) = (1, 0)$$

This gives us, the following two equations:

$$
\begin{aligned}
aa^{-1} - bb^{-1} &= 1 \\
ab^{-1} + ba^{-1} &= 0
\end{aligned}
$$

Solving yields $(a^{-1}, b^{-1}) = \left(\dfrac{a}{a^2+b^2}, \dfrac{-b}{a^2+b^2} \right)$.

$$(a^{-1}, b^{-1}) * (a, b) = (e_1, e_2) \ \Rightarrow (a^{-1}a - b^{-1}b, a^{-1}b + b^{-1}a) = (1, 0)$$

Solving also yields $(a^{-1}, b^{-1}) = \left(\dfrac{a}{a^2+b^2}, \dfrac{-b}{a^2+b^2} \right)$.

Therefore $(a, b) * (c, d) = (ac - bd, ad + bc)$, on the set $\mathbb{R} \times \mathbb{R}$ forms a group. It is also an abelian group as the operation is commutative:

$$(a, b) * (c, d) = (ac - bd, ad + bc) = (c, d) * (a, b) = (ca - db, cb + da)$$

5. Consider the operation of the preceding problem on the set $\mathbb{R} \times \mathbb{R}$. Is this a group? Explain.

Solution. This is not a group, as not every element has an inverse, since $(0, 0)^{-1}$ results in a division by zero and is therefore not in the set $\mathbb{R} \times \mathbb{R}$.

C. Groups of Subsets of a Set

1. Prove that there is an identity element with respect to the operation +, which is _____

Proof: Let $x \in P_D$. Then $x + \varnothing = x$ and $\varnothing + x = x$. Therefore $\varnothing$ is the identity element. ■

2. Prove every subset of A of D has an inverse with respect to +, which is _____ . Thus, $\langle P_D, + \rangle$ is a group!

Proof: Let $x \in P_D$. Then $x + x = \varnothing$. Therefore every element is its own inverse. ■

3. Let D be the three-element set $D = \{a, b, c\}$. List the elements of P_D. Then write the operation table for $\langle P_D, +\rangle$.

Solution.

$$P_D = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

$*$	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{a\}$	a	$\varnothing$	$\{a,b\}$	$\{a,c\}$	$\{b\}$	$\{c\}$	$\{a,b,c\}$	$\{b,c\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{b,c\}$	$\{a\}$	$\{a,b,c\}$	$\{c\}$	$\{a,c\}$
$\{c\}$	$\{c\}$	$\{a,c\}$	$\{b,c\}$	$\varnothing$	$\{a,b,c\}$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\{a,b,c\}$	$\varnothing$	$\{b,c\}$	$\{a,c\}$	$\{c\}$
$\{a,c\}$	$\{a,c\}$	$\{c\}$	$\{a,b,c\}$	$\{a\}$	$\{b,c\}$	$\varnothing$	$\{a,b\}$	$\{b\}$
$\{b,c\}$	$\{b,c\}$	$\{a,b,c\}$	$\{c\}$	$\{b\}$	$\{a,c\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,c\}$	$\{a,b\}$	$\{c\}$	$\{b\}$	$\{a\}$	$\varnothing$

D. A Checkerboard Game

1. If $G = \{V, H, D, I\}$. and $*$ is the operation we have just described, write the table of G.

Solution.

$*$	V	H	D	I
V	I	D	H	V
H	D	I	V	H
D	H	V	I	D
I	V	H	D	I

2. Granting associativity, explain why $\langle G, *\rangle$ is a group.

Solution. We can see from the table that I is the identity element as any element multiplied by I results in that element. That every element is its own inverse since multiplying it by itself has the same result as staying put. Given that we are given the operation is associative, then we have met all the group axioms and therefore the operation * on the set G forms a group.

E. A Coin Game

1. If $G = \{I, M_1, \ldots, M_?\}$ and $*$ is the operation we have just described, write the table of $\langle G, * \rangle$.

Solution.

$*$	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	M_1	I	M_3	M_2	M_5	M_4	M_7	M_6
M_2	M_2	M_3	I	M_1	M_6	M_7	M_4	M_5
M_3	M_3	M_2	M_1	I	M_7	M_6	M_5	M_4
M_4	M_4	M_6	M_5	M_7	I	M_2	M_1	M_3
M_5	M_5	M_7	M_4	M_6	M_1	M_3	I	M_2
M_6	M_6	M_4	M_7	M_5	M_2	I	M_3	M_1
M_7	M_7	M_5	M_6	M_4	M_3	M_1	M_2	I

2. Granting associativity, explain why $\langle G, * \rangle$ is a group. Is it commutative? If no, show why not.

Solution. $\langle G, * \rangle$ is a group because it meets all the group axioms. The set G contains an identity element, I. From the table we can see that every element has an inverse, and we are given that its associative. Therefore the operation * on G forms a group. It is not a commutative group tho. As we can see from the table

$$M_1 * M_6 = M_7, \text{ but}$$

$$M_6 * M_1 = M_4$$

F. Groups in Binary Codes

1. Show that $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n)$.

Solution.

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$(b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n) + = (b_1 + a_1, b_2 + a_2, \ldots, b_n + a_n)$$

Since it was shown commutative for length 1, we therefore have $(a_i + b_i) = (b_i + a_i)$ and the above equations are equal.

2. To verify the associative law, we first verify it for words of length 1:

$$1 + (1 + 1) = 1 + 0 = 1 = 0 + 1 = (1 + 1) + 1$$

$$1 + (1 + 0) = 1 + 1 = 0 = 0 + 0 = (1 + 1) + 0$$

check the remaining six cases.

Solution.

$$\begin{array}{c}
1 + (0 + 1) = 1 + 1 = 0 = 1 + 1 = (1 + 0) + 1 \\
1 + (0 + 0) = 1 + 0 = 1 = 1 + 0 = (1 + 0) + 0 \\
0 + (1 + 1) = 0 + 0 = 0 = 1 + 1 = (0 + 1) + 1 \\
0 + (1 + 0) = 0 + 1 = 1 = 1 + 0 = (0 + 1) + 0 \\
0 + (0 + 1) = 0 + 1 = 1 = 0 + 1 = (0 + 0) + 1 \\
0 + (0 + 0) = 0 + 0 = 0 = 0 + 0 = (0 + 0) + 0
\end{array}$$

3. Show that $(a_1, \ldots, a_n) + [(b_1, \ldots, b_n) + (c_1, \ldots, c_n)] = [(a_1, \ldots, a_n) + (b_1, \ldots, b_n)] + (c_1, \ldots, c_n)$

Solution.

$$\begin{aligned}
(a_1, \ldots, a_n) + [(b_1, \ldots, b_n) + (c_1, \ldots, c_n)] &= (a_1, \ldots, a_n) + (b_1 + c_1, \ldots, b_n + c_n) \\
&= (a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n)
\end{aligned}$$

$$\begin{aligned}
[(a_1, \ldots, a_n) + (b_1, \ldots, b_n)] + (c_1, \ldots, c_n)] &= (a_1 + b_1, \ldots, a_n + b_n) + (c_1, \ldots, c_n) \\
&= (a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n)
\end{aligned}$$

4. The identity element of $\mathbb{B}^n$, that is, the identity element for adding words of length n, is _____

Solution.

$$(0_1, 0_2, \ldots, 0_n)$$

5. The inverse, with respect to word addition, of any word $(a_1, \ldots a_n)$ is

Solution. Every word is its own inverse,

$$(a_1, \ldots a_n)$$

6. Show that $a + b = a - b$ [where $a - b = a + (-b)$]

Solution. Since every word is its own inverse we have $-b = b$ and therefore

$$a - b = a + (-b) = a + b$$

7. If $a + b = c$, show that $a = b + c$.

Solution.

$$\begin{aligned} a + b &= c \\ a + b + b &= c + b \quad \text{via equality} \\ a + (b + b) &= c + b \quad \text{via associativity} \\ a + 0 &= c + b \quad \text{via inverse} \\ a &= c + b \quad \text{via identity} \end{aligned}$$

G. Theory of Coding: Maximum-Likelihood decoding

1. Verify that every codeword $a_1a_2a_3a_4a_5$ in C_1 satisfies the following two parity-check equations: $a_4 = a_1 + a_3$; $a_5 = a_1 + a_2 + a_3$.

Solution.

00000; 0 + 0 = 0, 0 + 0 + 0 = 0
00111; 0 + 1 = 1, 0 + 0 + 1 = 1
01001; 0 + 0 = 0, 0 + 1 + 0 = 1
01110; 0 + 1 = 1, 0 + 1 + 1 = 0
10011; 1 + 0 = 1, 1 + 0 + 0 = 1
10100; 1 + 1 = 0, 1 + 0 + 1 = 1
11010; 1 + 0 = 1, 1 + 1 + 0 = 1
11101; 1 + 1 = 0, 1 + 1 + 1 = 0

2. Let C_2 be the following code in $\mathbb{B}^6$. The first three positions are the information positions, and every codeword $a_1a_2a_3a_4a_5a_6$ satisfies the parity-check equations $a_4 = a_2, a_5 = a_1 + a_2$, and $a_6 = a_1 + a_2 + a_3$.

(a) List the codewords of C_2.
(b) Find the minimum distance of the code C_2.
(c) How many errors in any codeword of C_2 are sure to be detected? Explain.

Solution.
a) 000000, 001001, 010111, 011110, 100011, 101010, 110100, 111101

b) The minimum distance of C_2 is 2.

c) One errors is sure to be detected because it would transform a codeword into a noncodeword. However 2 errors could transform a codeword into another codword and thus is not guaranteed to be detected.

3. Design a code in $\mathbb{B}^4$ where the first two positions are information positions. Give the parity-check equations, list the codewords, and find the minimum distance.

Solution.

$$a_3 = a_0,\ a_4 = a_1 + a_2$$

$$C = \{0000, 0101, 1011, 1110\}$$

The minimum distance is 2.

4. Decode the following words in $c_1 : 11111, 00101, 11000, 10011, 10001$, and 10111.

Solution.

$$\begin{aligned} 11111 &\Rightarrow 11101 \\ 00101 &\Rightarrow 00111 \\ 11000 &\Rightarrow 11010 \\ 10011 &\Rightarrow 10011 \\ 10001 &\Rightarrow 10011 \\ 10111 &\Rightarrow 00111, 10011 \end{aligned}$$

5. Prove that it is possible to detect up to $m-1$ errors. (That is, if there are errors of transmission in $m-1$ or fewer positions of a codeword, it can always be determined that the received word is in correct.)

Proof: Assume for contradiction that it is not possible to detect an error of $m-1$ or fewer. Then we have a code in C that with $m-1$ or fewer errors can be transformed into another code in C so that we can not tell it contains an error. This is not possible since m is defined as minimum number of differences between any two pairs in C. $\rightarrow\!\leftarrow$

6. By the *sphere of radius k* about a codeword a we mean the set of all words in $\mathbb{B}^n$ whose distance from a is no greater than k. This set is denoted by $S_k(a)$; hence

$$S_k(a) = \{x : d(a,x) \leq k\}$$

If $t = \frac{1}{2}(m-1)$, prove that any two spheres of radius t say $S_t(a)$ and $S_t(b)$, have no elements in common.

Proof: Assume for contradiction that two spheres of radius t, $S_t(a)$ and $S_t(b)$ have an element in common. So $x \in S_t(a)$ and $x \in S_t(b)$. This means that $d(a,x) \leq \frac{m-1}{2}$ and $d(b,x) \leq \frac{m-1}{2}$ via definition of t. Thus $d(a,b) \leq d(a,x) + d(b,x) \Rightarrow d(a,b) \leq m-1$. This leads to a contradiction as m is defined to be the smallest distance between any two codewords. Therefore any two spheres of radius t have no elements in common. ■

7. Deduce from part 6 that if there are t or fewer errors of transmission in a codeword, the received word will be decoded correctly.

Solution. Since any $x \in \mathbb{B}^n$ can not lie in more than one sphere of radius t, any x with t or fewer errors can be correctly decoded to the codeword whose sphere it resides in.

8. Let C_2 be the code described in part 2. Using the results of parts 5 and 7, explain why two errors in any codeword can always be detected, and why one error in any codeword can always be corrected.

Solution. This is not true, since the minimum distance of C_2 was two, two errors in a codeword can transform it into another codeword and therefore make it impossible to detect there were errors. Furthermore via part 7 we have $t = \frac{2-1}{2} = \frac{1}{2}$ and so a single error can not be guaranteed to be decoded correctly. For example 000001 could be either 000000 or 001001.