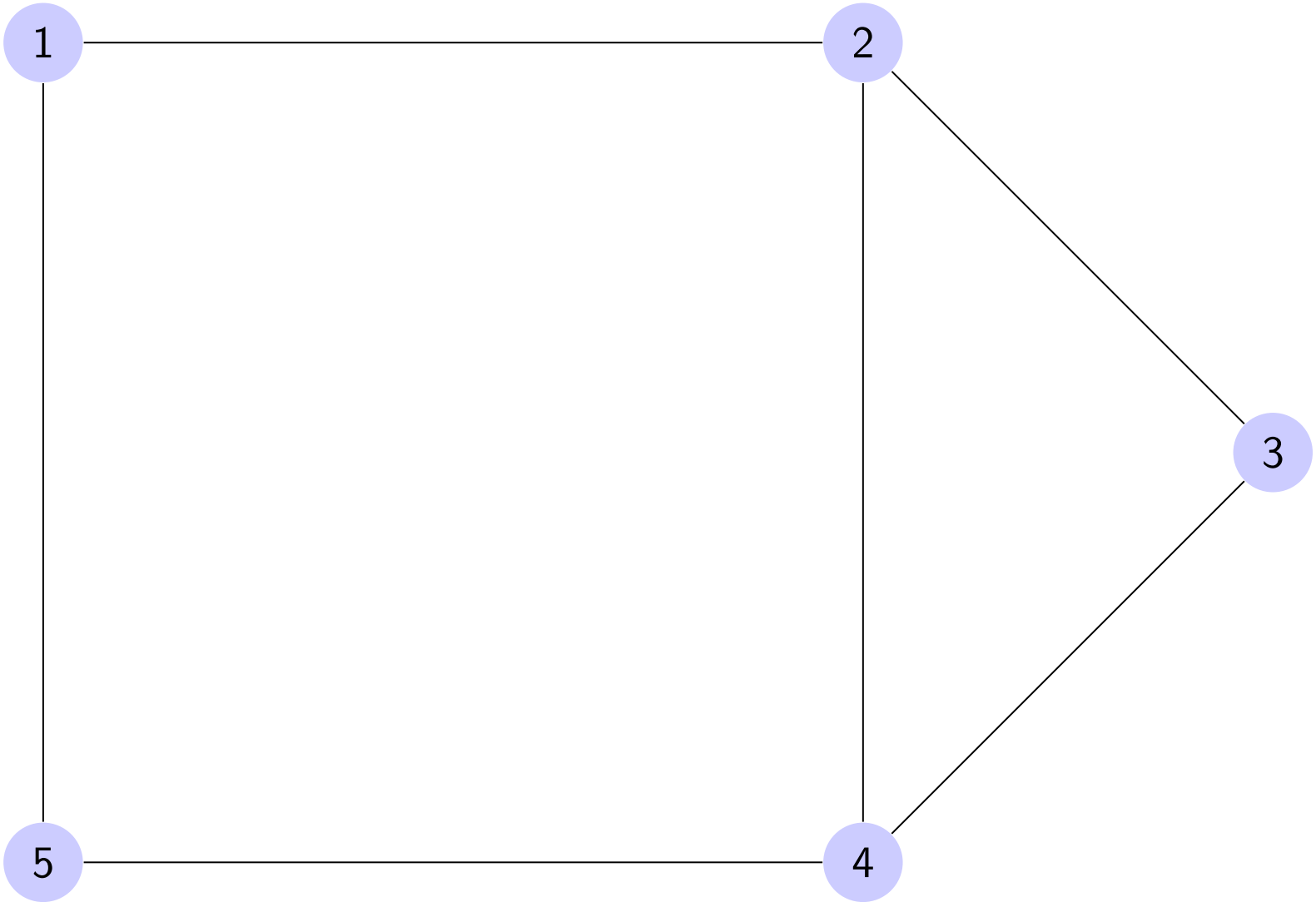
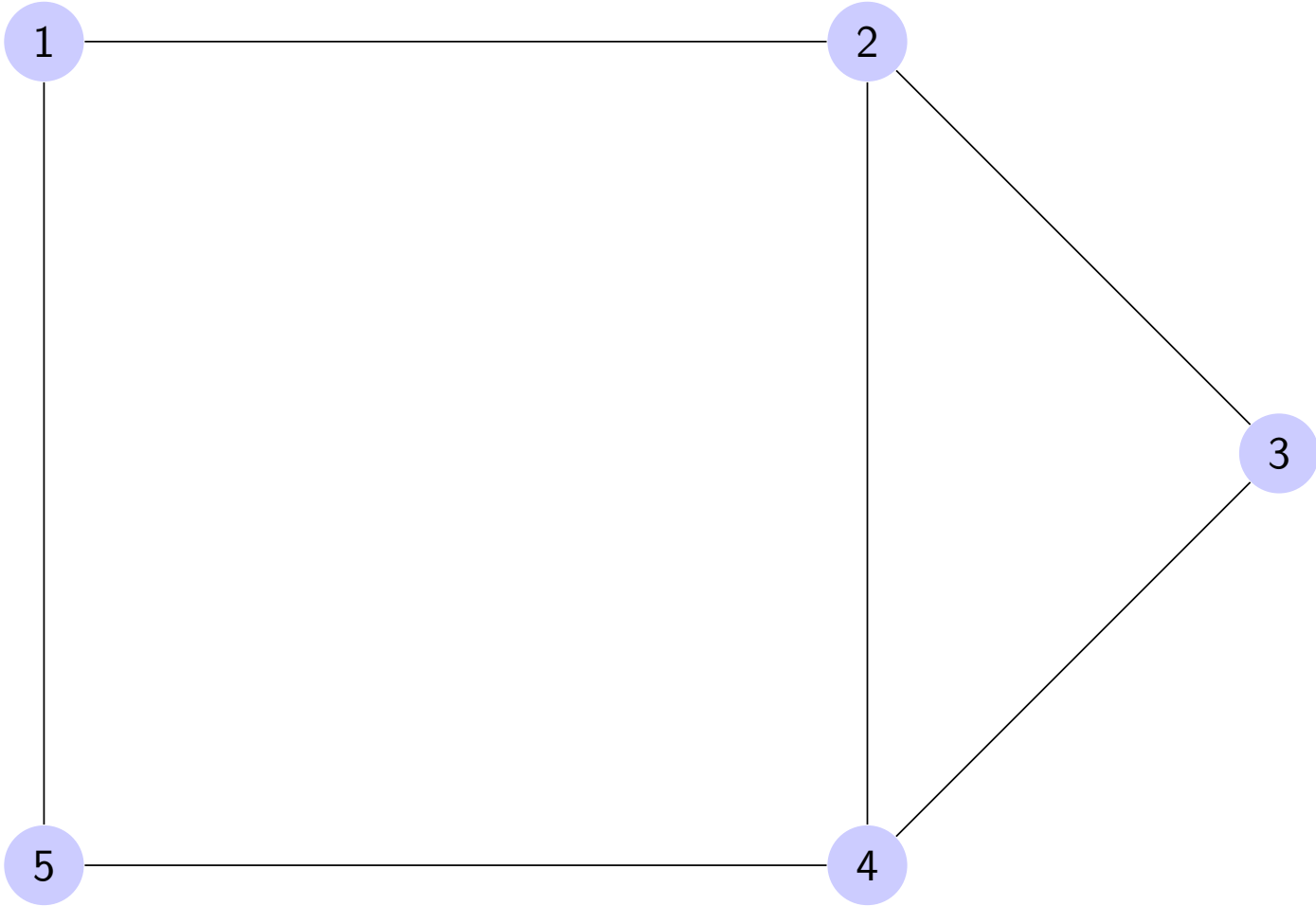
MA294 - Problems

July 28, 2021

21.2-1

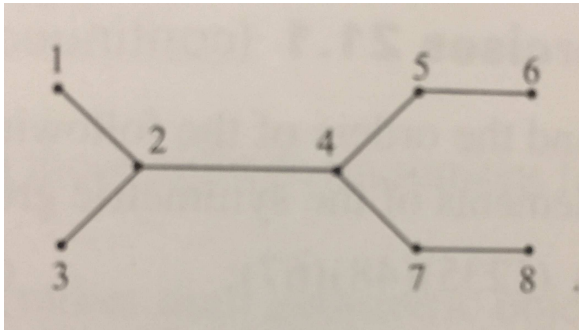
Determine $Aut(\Gamma)$ for the graph Γ:





The book claims that $|Aut(\Gamma)| = 2$ and indeed this is the case.
If $\sigma \in Aut(\Gamma)$ then $\sigma(2) = 2$ (and $\sigma(4) = 4$) or $\sigma(2) = 4$ (and therfore $\sigma(4) = 2$) as these are the only nodes that are degree 3.
Thus $\sigma(3) = 3$ as $2 \leftrightarrow 3$ and $4 \leftrightarrow 3$.
And if $\sigma(2) = 4$ then $\sigma(1) = 5$ and $\sigma(5) = 1$, moreover, if $\sigma(2) = 2$ and $\sigma(4) = 4$ then $\sigma(1) = 1$ and $\sigma(5) = 5$.
So $Aut(\Gamma) = \{(), (2,4)(1,5)\}$.
Note that if $G = Aut(\Gamma)$ then the orbits are $G1 = \{1,5\}$, $G2 = \{2,4\}$ and $G3 = \{3\}$.

21.2-3

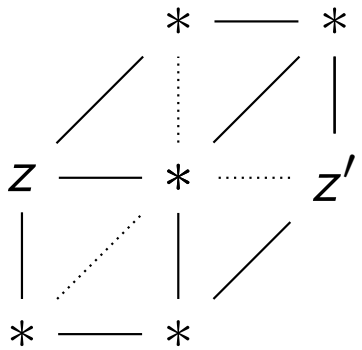


Since v_5 and v_7 and are the only nodes of degree two then if $\sigma \in Aut(\Gamma)$ then either $\sigma(5) = 5$ and $\sigma(7) = 7$ or $\sigma(5) = 7$ and $\sigma(7) = 5$. And if $\sigma(5) = 7$,$\sigma(7) = 5$ then $\sigma(6) = 8$,$\sigma(8) = 6$. This also implies that $\sigma(4) = 4$ and since $4 \leftrightarrow 2$ then $\sigma(2) = 2$.
As to the nodes 1 and 3 then basically, either $\sigma(1) = 3$,$\sigma(3) = 1$ or $\sigma(1) = 1$,$\sigma(3) = 3$ but this is independent of what σ does to $5, 6, 7, 8$.
Thus $Aut(\Gamma) = \{(), (1, 3), (5, 7)(6, 8), (1, 3)(5, 7)(6, 8)\}$ and thus the orbits are $\{1, 3\}, \{2\}, \{4\}, \{5, 7\}, \{6, 8\}$.

21.3-2

Let X denote the set of corners of a cube, and let G denote the group of permutations of X which correspond to rotations of the cube. Show that: (i) G has just one orbit on X. If we have any vertex on the 'top' of the cube, then by rotating any other vertex on the top is in the orbit. However, we can rotate around a different axis to move that vertex to another vertex on the same 'face' and indeed a given vertex can be rotated into any other vertex position and thus, for any vertex 'v', $Gv = X$.

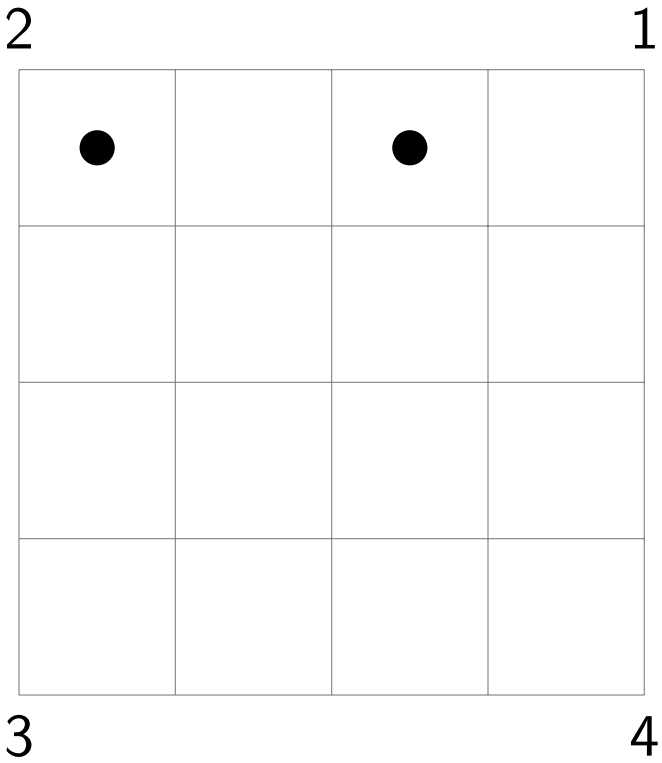
(ii) If z is any corner, the $|G_z| = 3$. To see this consider the rotation about the line through z to the corner z' diagonally *opposite*. About this axis you rotate three times until you get back to where you started, and each such rotation leaves this vertex alone, ergo $|G_z| = 3$.



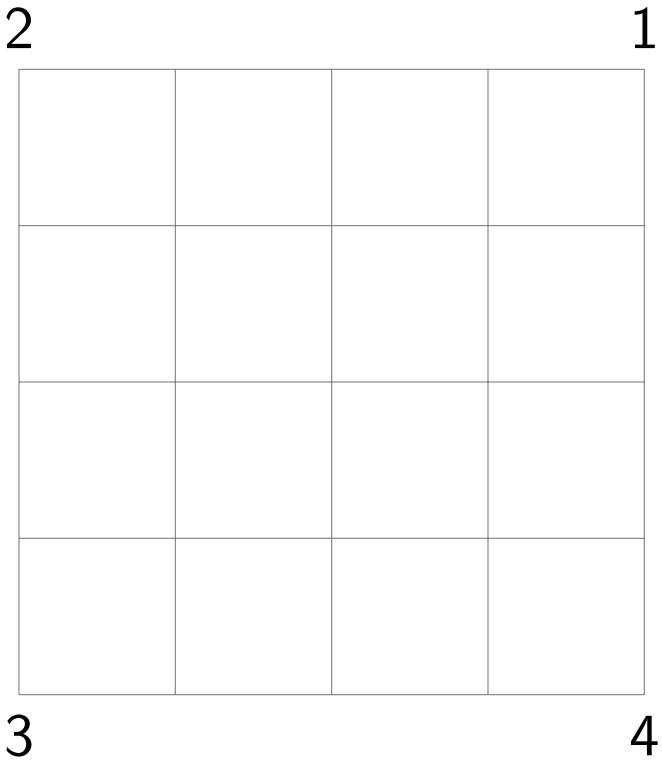
(iii) $|G| = 24$ - This is a nice consequence of the orbit stabilizer theorem, namely that $[G : G_z] = |Gz|$ where $[G : G_z] = \frac{|G|}{|G_z|}$ which yields $\frac{|G|}{3} = 8$ whence $|G| = 24$.

21.4-2

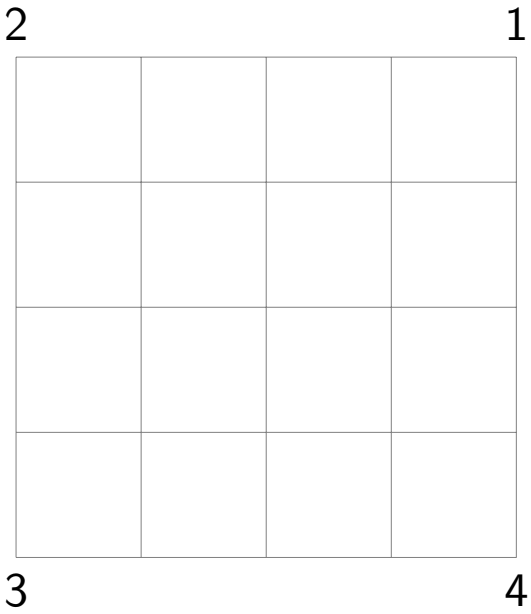
For a 4×4 card with two holes cut in such as this



we consider the action of $D_4 = \{r_0, r_{90}, r_{180}, r_{270}, f_{(1,2)}, f_{(2,3)}, f_{(1,3)}, f_{(2,4)}\}$

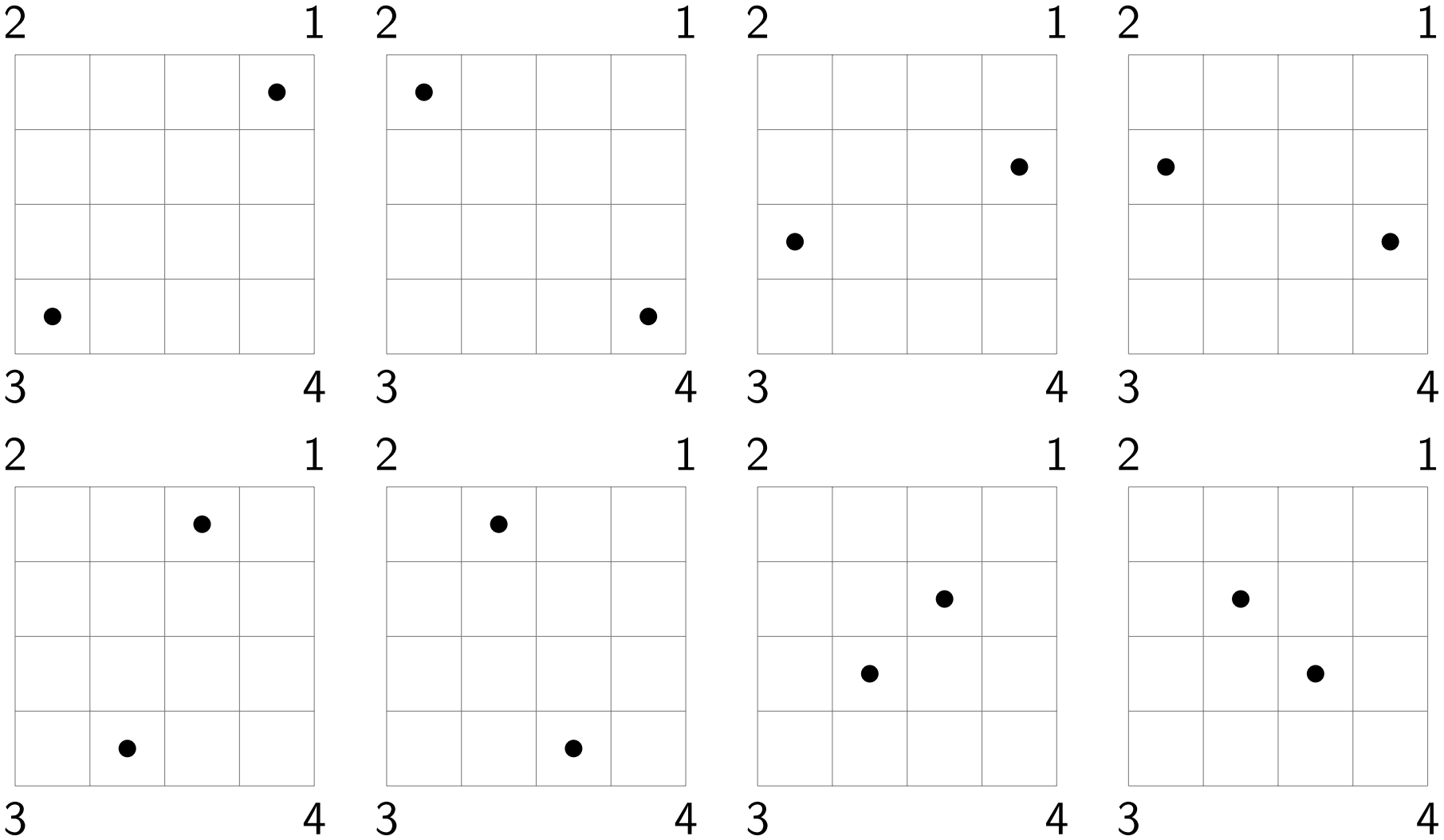


There are $\binom{16}{2} = 120$ different ways of punching the two holes in the grid, and we wish to use the formula $\frac{1}{|D_4|}\sum_{g\in D_4}|F(g)|$ where $F(g)$ is the set of configurations left fixed by $g \in D_4$.



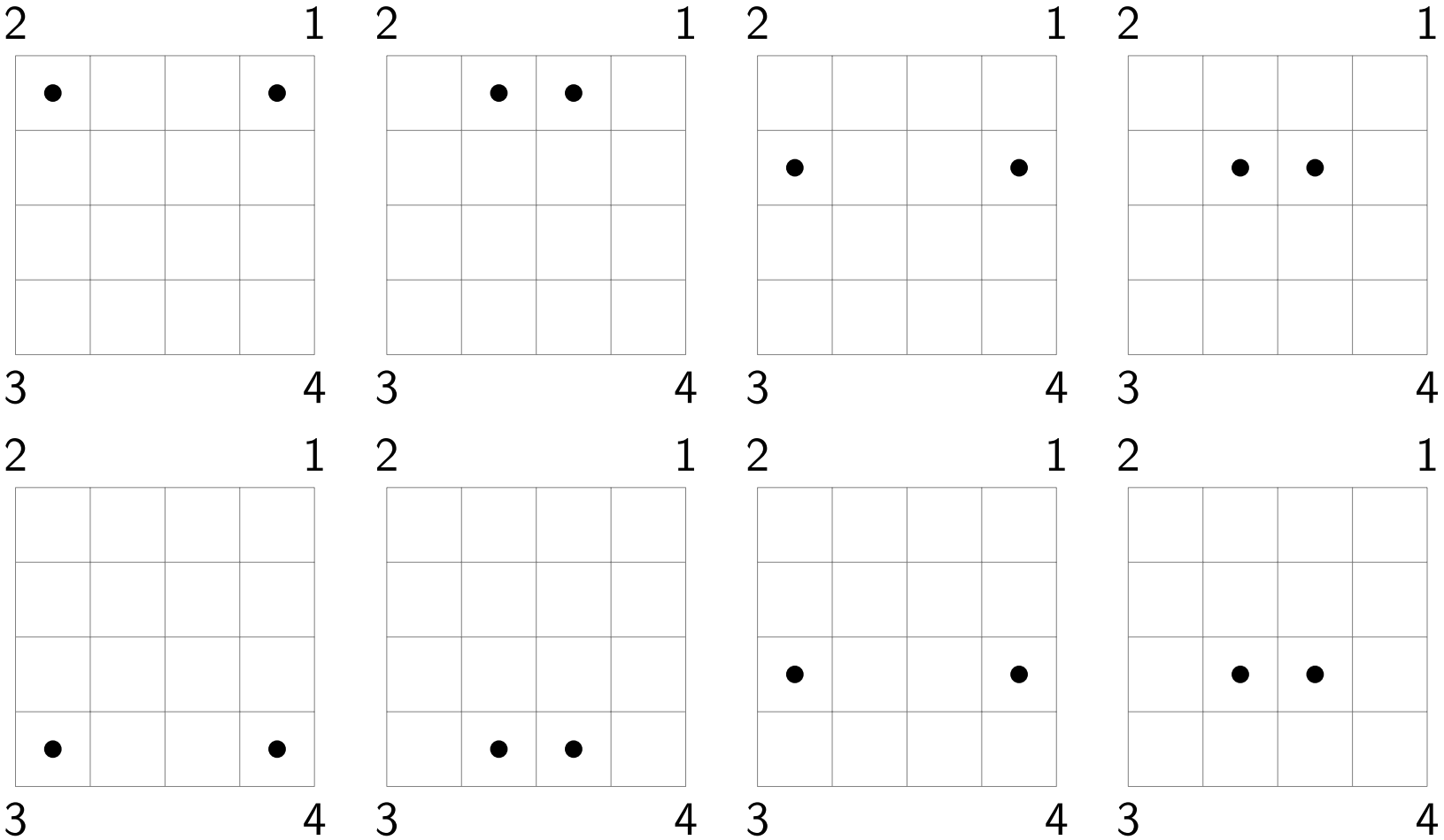
$|F(r_0)| = 120$ since all configurations are fixed by the identity.
$|F(r_{90})| = 0$ since there is no way to punch two holes such that a 90° turn moves a hole to a hole.
Similarly $|F(r_{270})| = 0$.

As to $|F(r_{180})|$ the vertices and sides of the square get exchanged, here are configurations which are preserved.



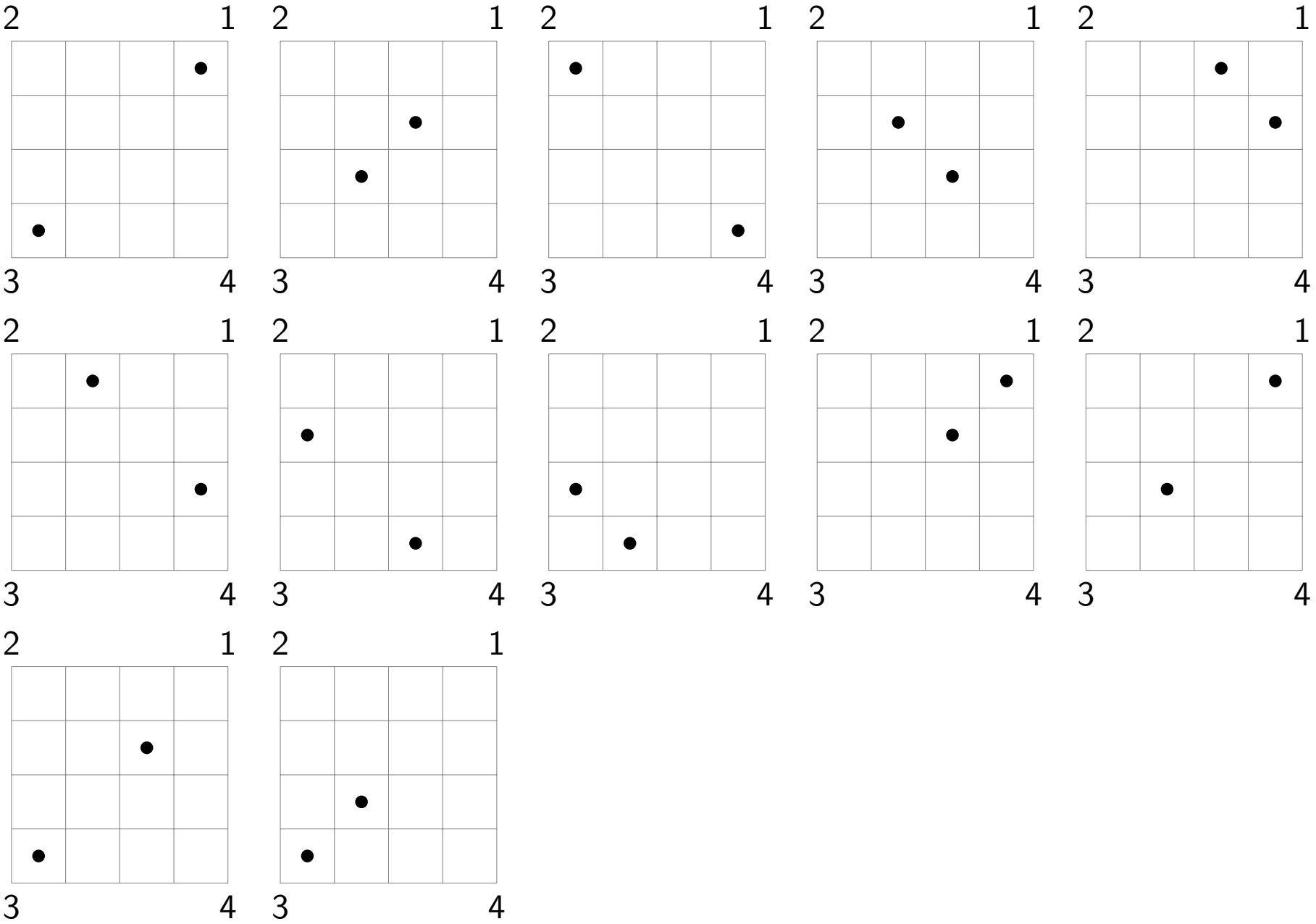
So $|F(r_{180})| = 8$.

As to $|F(f_{(1,2)})|$ the left and right sides get exchanged, here are configurations which are preserved.



So $|F(f_{(1,2)})| = 8$ and similarly $|F(f_{(2,3)})| = 8$

As to $|F(f_{(1,3)})|$ we have the following fixed configurations:



So $|F(f_{(1,3)})| = 10$ and similarly $|F(f_{(2,4)})| = 10$

So in summary the number of orbits is

$$\frac{1}{8}(120 + 0 + 8 + 0 + 8 + 8 + 10 + 10) = \frac{1}{8}(144) = 18$$

which is the number of distinct cards that can be made.

p.195#2

Let R be the ring of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

where $a, b \in \mathbb{R}$. Show that alhough R is a ring without unity, it contains a subring S with unity.

Since

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$$

then it's clear that R is a subring. If you look at the 'b' entry, it didn't appear in the product, so it's almost as if it could be left out, and indeed, if we consider matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ then

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix}$$

which clearly gives a subring, and you can check that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the multiplicative identity.

p.197#28
A ring R is a **Boolean** ring if $a^2 = a$ for all $a \in R$. Show that every Boolean ring is commutativ e.

Commutativity is the statement that $ab = ba$ for all $a, b \in R$.

For this one might think to try and do something with $(ab)^2$ and that $(ab)^2 = ab$ but this actually does n't give us much.

Instead, we observe that $ab = ba$ if $ab - ba = 0$ and consider $(a+b)^2 = (a+b)$ but this implies

$$\begin{aligned}
(a+b)^2 &= (a+b) \\
(a+b)(a+b) &= a+b \\
&\downarrow \text{ FOIL the left side} \\
a^2 + ab + ba + b^2 &= a+b \\
&\downarrow \\
a + ab + ba + b &= a+b \\
&\downarrow \text{ cancel } a \text{ and } b \\
ab + ba &= 0
\end{aligned}$$

So we're *almost there* in that $ab = -ba$ so the question is whether $-ba = ba$ and the answer is actuall y yes.

FACT: If R is a Boolean ring then $char(R) = 2$ actually.

Why?: Well $(a + a)^2 = (a + a)$ but this means $4a^2 = 2a$ but then $4a = 2a$ which means $2a = 0$.

As such $ba + ba = 0$ so $ba = -ba$ and so $ab = -ba$ implies $ab = ba$.

p.211#5a

Find all the zeros of $f(x) = 5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}$.

- $f(0) = 9$
- $f(1) = 17 = 5$
- $f(2) = 3$
- $f(3) = 9$
- $f(4) = 5$
- $f(5) = 9$
- $f(6) = 3$
- $f(7) = 5$
- $f(8) = 9$
- $f(9) = 9$
- $f(10) = 11$
- $f(11) = 9$

So $f(x)$ has **no** zeros in $\mathbb{Z}_{12}$.

p.212#10
Give two different factorizations of $f(x) = x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

We look for roots and find that $f(1) = 0$, $f(3) = 0$, and surprisingly that $f(6) = 0$ and $f(8) = 0$ which means that $(x-1)|f(x)$, $(x-3)|f(x)$, $(x-6)|f(x)$, and $(x-8)|f(x)$ so, in fact, we get these factorizations:

- $(x-1)(x-8) = x^2 - x - 8x + 8 = x^2 - 9x + 8 = x^2 + x + 8$
- $(x-3)(x-6) = x^2 - 6x - 3x + 18 = x^2 - 9x + 18 = x^2 + x + 8$

p.212#13
Show that the division algorithm fails in $\mathbb{Z}[x]$. Why does it fail?

Say $f(x) = 3x^2 + 1$ and $g(x) = 2x + 1$ then if $f(x) = q(x)g(x) + r(x)$ it must be that $q(x) = ax + b$ and $r(x) = c$ (a constant) which means

$$3x^2 + 1 = (2x + 1)(ax + b) + c$$
$$3x^2 + 1 = 2ax^2 + 2bx + ax + b + c$$
$$3x^2 + 1 = 2ax^2 + (2b + a)x + b + c$$

which leads us to the statement that $3 = 2a$ which is never true in $\mathbb{Z}$. The point is, we need to be able to divide coefficients to do long division, but in $\mathbb{Z}$ this maynot be possible, although it *would* work if we were in $\mathbb{Q}[x]$ for example.

24.1-1

Find the minimum distance δ for the code:
(i) $C = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$ As $0000 \in C$ then it's not hard to see that $\delta = 2$ since if you take any of the other codewords and change a bit from '0' to '1' (or vice-versa) then you would get a code with 3 bits equal to 1, but none of the code words has 3 bits equal to 1.
As such we conclude that this code could detect 1 error.

24.2-1

For any $n \geq 1$, the code containing just $00\ldots0$ and $11\ldots1$ is a linear code. What are the values of k and δ.
Well, $\delta = n$ since for a linear code, $\delta = w_{min}$ and here, this is the number of '1' bits in the codeword $11\ldots1$.
The value of k is basically $log_2(number\ of\ codewords)$ which in this case is 1.

24.2-2

Given any word $\vec{x} \in \mathbb{F}_2^n$, let $S_2(\vec{x})$ be the number of words obtained by making at most 2 errors in $\vec{x}$. Show that $|S_2(\vec{x})| = \frac{1}{2}(n^2 + n + 2)$.

This is basically $\binom{n}{0} + \binom{n}{1} + \binom{n}{2}$.

And this equals

$$\begin{aligned} 1 + n + \frac{n!}{2!(n-2)!} &= 1 + n + \frac{n(n-1)}{2} \\ &= 1 + n + \frac{n^2 - n}{2} \\ &= \frac{2 + 2n}{2} + \frac{n^2 - n}{2} \\ &= \frac{n^2 + n + 2}{2} \end{aligned}$$

24.3-3

Suppose we wish to be able to send 128 different messages, and each message is to be represented by a binary codeword of length 11. Explain how to construct a linear code for this purpose.
Here, our $n = 11$ and if we have a matrix H whose nullspace will yield this code, then H must have 11 columns, and, assuming H is row-reduced, we need $7 = log_2(128)$ free variables which means H is 4×11, with the form $H = \left[I_4 | M\right]$ where M is 4×7.

24.4-1

Let C be the linear code defined by the check matrix:

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

and one receives the codeword 110110, and only one error has been made, what is the intended codeword.
Simply multiply

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} a$$

which is the second column of the check matrix, which means the second bit is 0, i.e. the correct codeword is 100110.