Oppgaver

Seksjon 4

- Determine if the given set + operation form a group.

4.11

- All $n \times n$ diagonal matrices under addition:
  - Yes! We must show that the group axioms hold: (we do this for 2×2 matrices)
    - Associativity: $(M+N)+L \overset{?}{=} M+(N+L)$

$$\Bigg[\underbrace{\begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix}}_{M} + \underbrace{\begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix}}_{N}\Bigg] + \underbrace{\begin{pmatrix} l_1 & 0 \\ 0 & l_2 \end{pmatrix}}_{L}$$

$$= \left[\begin{pmatrix} m_1+n_1 & 0 \\ 0 & m_2+n_2 \end{pmatrix}\right] + \begin{pmatrix} l_1 & 0 \\ 0 & l_2 \end{pmatrix}$$

$$= \begin{pmatrix} m_1+n_1+l_1 & 0 \\ 0 & m_2+n_2+l_2 \end{pmatrix}.$$

We ~~see~~ that we get the same answer for the right hand side, hence associativity holds.

In fact, we could have seen this immediately, since the operation is inherited from $\mathbb{R}$, associativity hold automatically.

- Identity element We must find an element 0 such that $M + 0 = M = 0 + M$.

But this is trivial. We let $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ be the zero matrix.

- Inverses Again, these are inherited from $\mathbb{R}$. Explicitly, if $M = \begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix}$, then

$$-M = \begin{pmatrix} -m_1 & 0 \\ 0 & -m_2 \end{pmatrix}.$$

Hence the set of 2×2 diagonal matrices is a group under matrix addition. The exact same proofs work for the $n\times n$ case – there's just more notation.

4.13] • All $n\times n$ diagonal matrices w/ no zeros on the diagonal under matrix multiplication

This is again a group. The identity element is

$$I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

the matrix w/ only 1's on the diagonal.

4.12] • All $n\times n$ diagonal matrices under matrix multiplication.

This is not a group. The zero matrix have no inverse!

4.14 · All $n \times n$ diagonal matrices w/ only ± 1 on the diagonals. ③

Yeah, it's a group. (isomorphic to $(\mathbb{Z}/2)^n$)

4.15 · All $n \times n$ upper-triangular matrices under multiplication.

Not a group! (not all inverses exist)

4.16 · $n \times n$ upper triangular matrices under matrix addition.

It's a group! (isomorphic to $(\mathbb{R}^{\frac{(n+1)n}{2}}, +)$)

4.17 · $n \times n$, upper triangular matrices w/ det 1 under multiplication.

It's a group! This is matrix multiplication, so we know that associativity holds. The identity element is the identity matrix, so the only thing we need to show is that

① It's closed under multiplication.

② The inverses are also upper triangular.

We do ① first. Note that if we multiply a matrix M by $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, the answer is the ith column of M.

Hence:

$$MNe_i = M\begin{pmatrix} a_1\\ \vdots \\ a_i \\ 0 \\ \vdots \\ 0\end{pmatrix} = \begin{pmatrix} m_{11} & & \vdots & \\ & m & \vdots & \\ & & m_{ii} & \\ O & & & \ddots \end{pmatrix}\begin{pmatrix} a_1\\ \vdots\\ a_i\\ 0\\ \vdots\\ 0\end{pmatrix}$$

Since N is upper triangular

$$= \begin{pmatrix} m_1\\ \vdots \\ m_i \\ 0\\ 0\\ 0\\ 0\end{pmatrix} \leftarrow$$ check *yourself* why!

② The inverses are also upper triangular.

This is a little trickier to see. Recall that to find the inverse of a matrix you can use Gaussian elimination on the augmented matrix

$$\left(M \,\middle|\, I_n\right).$$

If M is upper-triangular, we are in the following situation:

$$\left(\begin{array}{cccc|cccc} m_{11} & m_{21} & \cdots & & 1 & 0 & & \\ 0 & m_{22} & & & 0 & 1 & & O \\ 0 & 0 & m_{33} & & \vdots & & 1 & \\ \vdots & \vdots & & \ddots & & & & \ddots \\ \vdots & \vdots & & & & O & & 1 \end{array}\right)$$

The next step is to divide the first row by m_{11}. Then we can get m_{21} away by subtracting a multiple of the second row:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & m_{31}' & \cdots & m_{11}^{-1} & -\frac{m_{21}}{m_{22}} & \cdots & \cdot \\ 0 & m_{22} & \cdots & & 0 & 1 & 0 & \cdots \\ & & m_{33} & & & & 1 & \\ & 0 & & \ddots & & 0 & & \ddots \; 1 \end{array}\right)$$

Now we can divide the second row by m_{22} to get a 1 there as well. Continuing this way, from top to bottom, we find the inverse of M without introducing any elements below the diagonal. Hence the inverse is also diagonal.

$\underline{4.18}$ • All $n \times n$ matrices w/ $\det M = \pm 1$.

The only thing we need to check is that the set is closed under multiplication and inverses.

① <u>Multiplication</u> If M, N have determinant ± 1, then

$$\det(MN) = \det M \cdot \det N = \pm 1 \cdot \pm 1 = \pm 1.$$

② <u>Inverses</u> If M^{-1} is the inverse of M, then

$$1 = \det(I) = \det(MN) = \det M \cdot \det M^{-1} = \pm \det M^{-1} \checkmark$$

Section 5

5.47 Prove that if G is an abelian group, then the set of all elements w/ $x^2 = e$ form a subgroup H of G.

(this is called the 2-torsion subgroup)

We check the conditions of Theorem 5.14

① H is closed under multiplication:

Let $x^2 = e$ and $y^2 = e$. Then $(xy)^2 = xyxy$

$= xxyy = ee = e$.

Note that we needed to use that G was abelian.

② The identity element e of G is in H.

Clearly $e^2 = e$.

③ If $a \in H$, then $a^{-1} \in H$ also.

Look at a^{-1}. Then $(a^{-1})^2 \underset{\uparrow \text{ by definition}}{=} a^{-2} = (a^2)^{-1} \underset{\uparrow\, a^2 = e}{=} e^{-1} = e$.

since $a^{-1}a^{-1}a^2 = a^{-1}a^{-1}aa = e$, and inverses are unique.

Hence H is a subgroup of G.

Section 8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}.$$

$\boxed{8.1}$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

$\boxed{8.2}$

$$\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}.$$

$\boxed{8.3}$

$$\mu\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}.$$

$\boxed{8.4}$

$$\sigma^{-2}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix}.$$

must look in
row 2 instead

$\boxed{8.5}$

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

8.46 Show that S_n is nonabelian for $n \geq 3$. (8)

We first show that S_3 is non-abelian.

Consider $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Then $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, but

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then we show that S_3 is a subgroup of S_n for $n \geq 3$.

Indeed, let $\sigma \in S_3$ as given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 & 5 & \cdots & n \end{pmatrix}$$

Then S_3 is realized as the subgroup of S_n leaving $(4, 5, \ldots, n)$ fixed, but permuting $(1, 2, 3)$.

Hence S_n have a non-abelian subgroup, which is not possible unless S_n is non-abelian itself.

Section 6

- Find the number of elements in the indicated cyclic group.

$\boxed{6.17}$ The cyclic subgroup of $\mathbb{Z}/30$ generated by 25.

We write the multiples of 25 modulo 30:

25, 20, 15, 10, 5, $\underset{\overset{\|}{0}}{30}$, so the order is 6.

We could have used Theorem 6.14 which said that the order is $\frac{30}{\gcd(25,30)} = \frac{30}{5} = \underline{\underline{6}}$.

$\boxed{6.18}$ $\langle 30 \rangle \leq \mathbb{Z}/42$. $\# \langle 30 \rangle = \frac{42}{\gcd(30,42)} = \frac{42}{6} = 7$.

Also 30, $\underset{\underset{\text{mod } 42}{30 \cdot 2}}{\overset{}{18}}$, 6, 36, 24, 12, $\underline{42 = 0 \text{ mod } 42}$

(samme svar ☺)

$\boxed{6.19}$ $i^2 = -1$, $i^3 = -i$, $i^4 = -i \cdot i = 1$

so $\langle i \rangle$ have 4 elements.

$\boxed{6.20}$ $\alpha = \frac{1+i}{\sqrt{2}} = e^{i\frac{\pi}{4}}$, so $\alpha^{8} = 1$. ← order

$\boxed{6.21}$ $|1+i| > 1$, so its powers can $\underline{\text{never}}$ be 1. Hence this subgroup is countably infinite. ($\cong \mathbb{Z}$)