We can represent permutations using **permutation matrices**. The key observation is that there is an obvious set bijection

$$[n] \cong \{e_1, e_2, \ldots, e_n\}.$$

Example 1.34. Let $\sigma = (1\ 3\ 2) \in S_3$. We can represent σ as the linear transformation that sends each $e_i \mapsto e_{\sigma(i)}$:

$$\sigma \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Recall from linear algebra the following two facts:

- The determinant of the $n \times n$ identity matrix $I_n \in M_{n\times n}(\mathbb{R})$ is 1.
- If M' is obtained from M by interchanging two different rows, then $\det A' = -\det A$.

Definition 1.35 (Sign of a permutation)**.** Let $p \in S_n$ be a permutation. The **sign** of p is equal to the determinant of the permutation matrix P representing p:

$$\operatorname{sgn}(p) := \det(P).$$

The following exercise shows we could equivalently define $\operatorname{sgn}(p)$ to be $(-1)^k$, where k is the number of transpositions in any composition of transpositions equal to p. If $\operatorname{sgn}(p) = +1$, we say that p is **even**; otherwise, if $\operatorname{sgn}(p) = -1$, we say that p is **odd**.

Exercise 1.36. (a) Prove that the transpose of a permutation matrix is its inverse.

(b) Prove that the determinant of a permutation matrix is always ± 1.

(c) Let $p \in S_n$, and write p as a composition (or equivalently, product) of k transpositions:

$$p = \tau_{i_1} \circ \tau_{i_2} \circ \ldots \circ \tau_{i_k}$$

Prove that p is even if and only if k is even, and that p is odd if and only if k is odd.

1.5 Complex numbers

The complex numbers $\mathbb{C}$ are is pervasive in mathematics and will provide us with many interesting examples of groups.

Let i be a variable satisyfing the relation $i^2 = -1$. The underlying set of $\mathbb{C}$ is $\{a + bi \mid a, b \in \mathbb{R}$. In other words, the complex numbers are just polynomials (with real coefficients) in the variable i, except that any time you see i^2, you can replace it with $-1 \in \mathbb{R}$.

This tells us how to add and multiply complex numbers. Addition is the same as vector addition in $\mathbb{R}^2$:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplication is the same as for polynomials:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

What's more interesting is that one can also divide complex numbers. That is, every nonzero complex number has a *multiplicative inverse*:

$$\frac{1}{a + bi} = (a + bi)^{-1} = \frac{1}{a^2 + b^2}(a - bi)$$

The variable of choice for complex numbers is usually z, followed by w. The **complex conjugate** of $z = a + bi$ is $\bar{z} = a - bi$.[4]

When we view z as a vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$, its length is given by $||z|| = \sqrt{a^2 + b^2}$. When we view z as a complex number, we call this the **absolute value** or **modulus** of z, and write

$$|z| = \sqrt{a^2 + b^2}.$$

[4]This is in analogy with the conjugates we learn about in precalculus: $a \pm b\sqrt{k}$.

Exercise 1.37. Verify that $z\bar{z} = |z|^2 = a^2 + b^2$, and observe that

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

It is often easier to work with polar coordinates (r, θ) rather than rectangular coordinates (x, y). We can write any complex number $z = x + iy$ in polar coordinates (r, θ) where

- $r = |z|$, the length of the vector z
- θ is the angle the vector z makes with the real axis (which is identified with the x-axis in $\mathbb{R}^2$).

Recall from precalculus that to translate from (r, θ) to (x, y), we compute

$$x = r\cos\theta \qquad y = r\sin\theta.$$

For Taylor series reasons, we can write

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Euler's formula says that $e^{\pi i} = -1$, and therefore $e^{2\pi i} = 1$.

Therefore if $z = x + iy$, and (x, y) in rectangular coordinates translates to (r, θ) in polar coordinates, we can write

$$z = x + iy = re^{i\theta}.$$

We will use this notation *extensively*, because it makes complex multiplication very simple. Let $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$. Then

$$z_1 z_2 = \left(r_1 e^{i\theta_1}\right)\left(r_2 e^{i\theta_2}\right) = (r_1 r_2)e^{(\theta_1+\theta_2)i}.$$

Geometrically, multiplication by i represents rotating by $\pi/2$ counterclockwise (CCW). That is, the vector iz is just the vector z rotated by $\pi/2$.

Example 1.38. The unit circle S^1 inside $\mathbb{C}$ is the set of complex numbers of modulus 1:

$$S^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}.$$

Note that I could have also written $\theta \in [0, 2\pi)$, or any other interval of this shape of length 2π, because $e^{2\pi i} = 1$.

This is a group under complex multiplication. (See HW01 for the same group described in a different way.)

Exercise 1.39. Prove that the **circle group** S^1 (under complex multiplication) is *not* cyclic.

Exercise 1.40. Prove that $\mathbb{C}^\times = \mathbb{C} - \{0\}$ is a group under complex multiplication.

Exercise 1.41. Find a *representation* of $\mathbb{C}^\times$ in $GL_2(\mathbb{R})$. That is, assign every element $z \in \mathbb{C}^\times = \mathbb{C} - \{0\}$ to a 2×2 invertible matrix so that matrix multiplication agrees with multiplication in $\mathbb{C}^\times$.

1.6 Aside: Real algebras

Here's an interesting nonabelian group.

Definition 1.42. The **quaternion group** H is the group consisting of elements

$$\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}.$$

where ± 1 commutes with all elements, and multiplication is determined by

$$\begin{aligned}
&\pm 1\mathbf{i} = \pm\mathbf{i}, \qquad \pm 1\mathbf{j} = \pm\mathbf{j}, \qquad \pm 1\mathbf{k} = \pm\mathbf{k} \\
&\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \\
&\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.
\end{aligned}$$

Remark 1.43. This construction of $\mathbb{C}$ from polynomials with real coefficients makes $\mathbb{C}$ into a real *algebra*[5]. We can keep going, and define the quaternions $\mathbb{H}$ and the octonions $\mathbb{O}$. However, the quaternions aren't commutative, and the octonions aren't even associative.

Exercise 1.44. (Advanced)

1. Define the *Hamiltonian quaternions* $\mathbb{H}$ as polynomials in $\mathbf{i}, \mathbf{j}, \mathbf{k}$ with real coefficient, subject to the relations in the group H. This makes $\mathbb{H} = \mathbb{R}[H]$, the *group ring* built from $\mathbb{R}$ and H. (We will talk more about rings later in the course.)

2. Define $\mathbb{H}$ differently, now using $\mathbb{C}$ as the coefficients. (This describes $\mathbb{H}$ as an algebra over $\mathbb{C}$.)

3. Use the description of $\mathbb{H}$ as an algebra over $\mathbb{C}$ to find a representation of $\mathbb{H}$ by 2×2 matrices with complex entries.

1.7 Subgroups

Definition 1.45. A subset H of a group G is a **subgroup** (written $H \leq G$) if it has the following properties:

- *Closure*: If $a, b \in H$, then $ab \in H$ as well.
- *Identity*: $1 = 1_G \in H$
- *Inverses*: If $a \in H$, then $a^{-1} \in H$ as well.

Example 1.46. The *even integers* $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$ is a proper subgroup of $\mathbb{Z}$.
Similarly, for any $n \in \mathbb{N}$, the set of multiples of n, denoted $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$, is a subgroup of $\mathbb{Z}$. (Note that $1\mathbb{Z} = \mathbb{Z}$ is not a proper subgroup.)

Warning The book writes $\mathbb{Z}n$ instead of $n\mathbb{Z}$, and hence writes the group $\mathbb{Z}/12\mathbb{Z}$ as $\mathbb{Z}/\mathbb{Z}12$. Either notation is mathematically reasonable, since $\mathbb{Z}$ is commutative. However, I prefer the more common notation $\mathbb{Z}/12\mathbb{Z}$.

Exercise 1.47. Convince yourself that for natural numbers $n, m \in \mathbb{N}$, $(nm)\mathbb{Z}$ is a subgroup of both $m\mathbb{Z}$ and $n\mathbb{Z}$. It may help to start with an example, e.g. $n = 2, m = 3$.

Example 1.48. The **trivial group** is the group with one element, the identity. Any nontrivial group G automatically has at least two subgroups:

1. the **trivial subgroup** $H = \{1\} \leq G$
2. $H = G$, the whole group itself.

A subgroup $H \leq G$ where $H \neq G$ (as a set) is called a **proper subgroup.**
A group G that has no nontrivial, proper subgroups is called a **simple group.**

Example 1.49. Here are some more examples of subgroups.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, where the group operation is $+$
2. $S^1 \leq (\mathbb{C}, \cdot)$
3. $S_k \leq S_n$ where $k \leq n$ ($k, n \in \mathbb{N}$)

The following proposition gives a potentially easier way to check whether a subset $H \subset G$ is a subgroup.[6]

Proposition 1.50. (The Subgroup Criterion) A subset H of a group G is a subgroup if and only if $H \neq \emptyset$ and for all $a, b \in H$, $ab^{-1} \in H$.

Exercise 1.51. Prove Proposition 1.50.

[5] This is a term we haven't defined yet.
[6] However, I often still just check the conditions in the definition.