Some aspects of group theory

# 1 Some examples of finite groups

Our goal in this section will be to collect some standard examples of finite groups. The main emphasis will be on realizing them as subgroups of $GL(n,\mathbb{R})$ or $GL(n,\mathbb{C})$.

**Cyclic groups:** For a natural number $n$, let $\mathbb{Z}/n\mathbb{Z}$ be the standard cyclic group of order $n$. We denote its elements by $0, 1, \dots, n-1$, and 1 is a generator. Another model for the cyclic group of order $n$ is the $n^{\text{th}}$ roots of unity, often denoted by $\mu_n$:

$$\mu_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\} = \{e^{2\pi ik/n} : k = 0, \dots, n-1\}.$$

Thus $\mu_n$ is a subgroup of the group $\mathbb{C}^*$ under multiplication, in fact of the group $U(1)$ of complex numbers of absolute value 1, and the function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mu_n$ defined by $f(k) = e^{2\pi ik/n}$ is an isomorphism.

**Cyclic groups and dihedral groups as rotation groups:** We first recall the description of elements of $O(2)$, the orthogonal group of $2\times 2$ matrices given in class and in Problem 1 of HW 3. Let $A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ and let $B_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ be $2\times 2$ orthogonal matrices (depending on a real number $\theta$ mod $2\pi$), with $\det A_\theta = 1$ and $\det B_\theta = -1$. Finally, let $R = B_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We will use without comment various identities whose proofs are part of Problem 1 of HW 3.

It is easy to see that $A_\theta$ is a counterclockwise rotation of the plane by the angle $\theta$, and that $A_{\theta_1} \cdot A_{\theta_2} = A_{\theta_1+\theta_2}$. In particular, $A_{2\pi/n}$ has order $n$, since $A^n_{2\pi/n} = A_{2\pi} = A_0 = \mathrm{Id}$. Thus the cyclic subgroup of $SO(2)$ generated by $A_{2\pi/n}$, i.e.

$$\langle A_{2\pi/n}\rangle = \{A_{2k\pi/n} : n = 0, \dots, n-1\},$$

has order $n$ and is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. This realization of $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of the rotation group is really the same as the realization of $\mathbb{Z}/n\mathbb{Z}$ as the subgroup $\mu_n$ of $U(1)$. In fact, viewing $\mathbb{C}$ as $\mathbb{R}^2$ with basis 1 corresponding to $e_1$ and $i$ corresponding to $e_2$, multiplication by the complex number $a+bi$ defines an $\mathbb{R}$-linear map $\mathbb{R}^2 \to \mathbb{R}^2$, whose corresponding matrix (with respect to the basis $1, i$) is $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Since $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2+b^2 = |a+bi|^2$, $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in SO(2)$ if and only if it is in $O(2)$, if and only if $a+bi$ has absolute value 1. Applying the above to $a+bi = e^{2\pi ki/n}$ identifies $\mu_n$ with $\langle A_{2\pi/n}\rangle$.

We turn now to $D_n$. For a natural number $n \geq 3$, let

$$\mathbf{p}_k = \left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right) \in \mathbb{R}^2.$$

It is easy to check that $\mathbf{p}_0 = (1,0), \mathbf{p}_1, \dots, \mathbf{p}_{n-1}$ are the vertices of a regular $n$-gon $P$ inscribed in the unit circle. They correspond to the elements of $\mu_n$ under the identification of $\mathbb{R}^2$ with $\mathbb{C}$. If $T$ is a symmetry of the $n$-gon $P$, then there exists a $k$ such that $T = A_{2k\pi/n}$ or $T = B_{2k\pi/n}$ in the above notation. In fact, since $T\mathbf{p}_0 = \mathbf{p}_k$ for some $k$, we know that the first column of $T$ must be $\mathbf{p}_k$, and then there are two possibilities for the second, $T = A_{2k\pi/n}$ or $T = B_{2k\pi/n}$. Conversely, if $T = A_{2k\pi/n}$ or $T = B_{2k\pi/n}$, then, for all $j$, $T\mathbf{p}_j = \mathbf{p}_\ell$ for some $\ell$ and hence $T$ is a symmetry of $P$. This can be checked by first checking it for for $T = A_{2k\pi/n}$, then for $T = B_0 = R$, then using $B_\theta = A_\theta R$. This shows that $D_n$ is isomorphic to the subgroup

$$\{A_{2k\pi/n}, B_{2k\pi/n} : k = 0, \dots, n-1\}$$

of $O(2)$. With $\rho = A_{2\pi/n}$ and $\tau = B_0 = R$, the cyclic subgroup $\langle\rho\rangle$ is equal to $\{A_{2k\pi/n} : k = 0, \dots, n-1\}$, and we have the identity $\tau\rho\tau = \rho^{-1} = \rho^{n-1}$. Thus $\rho$ and $\tau$ generate $D_n$, i.e. that every element of $D_n$ can be expressed in terms of $\rho$ and $\tau$. In fact, every element of $D_n$ can be uniquely written as $\rho^k\tau^a$, where $0 \leq k \leq n-1$ and $a$ is either 0 or 1. Using Problem 1 of HW 3, or similar methods, it is easy to work out the multiplication table for $D_n$ (all sums and differences of $k_1$ and $k_2$ are taken mod $n$): $\rho^{k_1}\rho^{k_2} = \rho^{k_1+k_2}$, $\rho^{k_1}(\rho^{k_2}\tau) = \rho^{k_1+k_2}\tau$, $(\rho^{k_1}\tau)(\rho^{k_2}) = \rho^{k_1-k_2}\tau$, $(\rho^{k_1}\tau)(\rho^{k_2}\tau) = \rho^{k_1-k_2}$.

Note that we can view $A_{2k\pi/n}$ as the (complex) linear map $\mathbb{C} \to \mathbb{C}$ given by multiplication by $e^{2\pi ik/n}$. The map $R$ can also be viewed as a map $\mathbb{C} \to \mathbb{C}$, namely $z \mapsto \bar{z}$. This map is $\mathbb{R}$-linear if we view $\mathbb{C}$ as an $\mathbb{R}$-vector space of dimension two with basis $1, i$, but of course it is not $\mathbb{C}$-linear.

**The quaternion group:** If $\mathbb{H}$ is the ring of quaternions, then since $\mathbb{H}$ is a division algebra its nonzero elements $\mathbb{H}^*$ are a group under multiplication. We can define the quaternion group $Q$ as a subgroup of $\mathbb{H}^*$:

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

We can also find $Q$ as a subgroup of $GL_2(\mathbb{C})$. Consider the following matrices in $M_2(\mathbb{C})$ (the $2 \times 2$ matrices with complex coefficients):

$$\mathbb{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \qquad \mathbb{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \qquad \mathbb{K} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

A computation shows that:

$$\mathbb{I}^2 = \mathbb{J}^2 = \mathbb{K}^2 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -\operatorname{Id}; \qquad \mathbb{I}\mathbb{J} = \mathbb{K}; \quad \mathbb{J}\mathbb{K} = \mathbb{I}; \quad \mathbb{K}\mathbb{I} = \mathbb{J}.$$

Then, using $\mathbb{I}^{-1} = -\mathbb{I}$, and similarly for $\mathbb{J}$, $\mathbb{K}$, and use: $(\mathbb{I}\mathbb{J})^{-1} = \mathbb{J}^{-1}\mathbb{I}^{-1}$ etc., it is easy to see that $\mathbb{J}\mathbb{I} = -\mathbb{K}$, $\mathbb{K}\mathbb{J} = -\mathbb{I}$, $\mathbb{I}\mathbb{K} = -\mathbb{J}$.

Thus $\{\pm\operatorname{Id}, \pm\mathbb{I}, \pm\mathbb{J}, \pm\mathbb{K}\}$ is a subset of $GL_2(\mathbb{C})$ (the invertible $2\times 2$ matrices with complex coefficients), and it is closed under matrix multiplication, contains Id, and contains the inverse of every element, so it is a subgroup of $GL_2(\mathbb{C})$, clearly isomorphic to $Q$. (As usual, associativity is automatic.)

In fact, we can also realize $Q$ as a subgroup of $GL(4, \mathbb{R})$. However, we shall not do so here.

**The symmetric and alternating groups:** We recall standard terminology and facts about $S_n$. Recall that $\#(S_n) = n!$.

**Definition 1.1.** Let $A = \{a_1, \dots, a_k\}$ be a subset of $\{1, \dots, n\}$ with exactly $k$ elements (i.e. for $i \neq j$, $a_i \neq a_j$). Consider the following element $\sigma$ of $S_n$. For $1 \leq i \leq k-1$, $\sigma(a_i) = a_{i+1}$, $\sigma(a_k) = a_1$, and $\sigma(j) = j$ if $j \notin A$. We call $\sigma$ a *$k$-cycle* and denote it by $\sigma = (a_1, \dots, a_k)$. Note that $\sigma$ depends on the **order** of the $a_i$ and not just on the **set** $A$. We call $\sigma$ a *cycle* if it is a $k$-cycle for some $k$ and refer to $k$ as the *length* of $\sigma$. A 1-cycle is always the identity. A 2-cycle is called a *transposition*. For $k \geq 2$, with $A$ and $\sigma$ as above, the set $A$ is called the *support* of $\sigma$, and written $\operatorname{Supp}\sigma$. It is the set of $i \in \{1, \dots, n\}$ such that $\sigma(i) \neq i$.

There are the following useful facts about $k$-cycles:

(i) $(a_1, a_2, \dots, a_k) = (a_2, a_3, \dots, a_k, a_1) = \cdots = (a_k, a_1, \dots, a_{k-1})$.

(ii) The order of a $k$-cycle $\sigma = (a_1, a_2, \dots, a_k)$ is $k$, and $\sigma^i(a_j) = a_{i+j}$, if $i + j \leq k$, and $\sigma^i(a_j) = a_{i+j-k}$, if $i + j > k$. (But, if $\sigma$ is a $k$-cycle, then $\sigma^r$ need not always be a $k$-cycle.) In particular, $\sigma^i(a_1) = a_{i+1}$ if $1 \leq i \leq k - 1$, and $\sigma^k(a_1) = a_1$.

(iii) $(a_1, a_2, \dots, a_k)^{-1} = (a_k, a_{k-1}, \dots, a_1)$.

(iv) Let $\sigma$ be a $k$-cycle and $\tau$ an $\ell$-cycle. We call $\sigma$ and $\tau$ *disjoint* if their supports are disjoint subsets of $\{1, \dots, n\}$, i.e. if $\operatorname{Supp} \sigma \cap \operatorname{Supp} \tau = \emptyset$. If $\sigma$ and $\tau$ are disjoint, then they commute, i.e. $\sigma\tau = \tau\sigma$.

(v) Given a $k$-cycle $(a_1, a_2, \dots, a_k)$ and an arbitrary element $\rho \in S_n$,

$$\rho \cdot (a_1, a_2, \dots, a_k) \cdot \rho^{-1} = (\rho(a_1), \rho(a_2), \dots, \rho(a_k)).$$

For a general $\sigma \in S_n$, we haves:

**Theorem 1.2.** *Let $\sigma \in S_n$. Then $\sigma$ is a product of disjoint cycles of lengths $\geq 2$. The expression of $\sigma$ as such a product is unique up to order.* $\square$

Let $(a_1, a_2, \dots, a_k)$ be a $k$-cycle. By direct computation, $(a_1, a_2, \dots, a_k)$ is a product of $k - 1$ transpositions:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2).$$

**Corollary 1.3.** *Every element of $S_n$ is a product of transpositions.* $\square$

**Theorem 1.4.** *Let $\sigma \in S_n$. If $\sigma = \tau_1 \cdots \tau_k = \rho_1 \cdots \rho_\ell$, where the $\tau_i$ and $\rho_j$ are all transpositions, then $k \equiv \ell \bmod 2$. In other words, $\sigma$ cannot be written both as a product of an even number of transpositions and a product of an odd number of transpositions.* $\square$

**Definition 1.5.** A permutation $\sigma \in S_n$ is *even* if $\sigma$ is a product of an even number of transpositions and *odd* if $\sigma$ is a product of an odd number of transpositions. The *sign* of a permutation $\sigma \in S_n$, $\varepsilon(\sigma)$ or $\operatorname{sgn} \sigma$, is $+1$ if $\sigma$ is even and $-1$ if $\sigma$ is odd. For $\sigma_1, \sigma_2 \in S_n$, $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$. Thus $\varepsilon$ is a homomorphism from $S_n$ to the multiplicative group $\{\pm 1\}$, and it is clearly surjective if $n \geq 2$. If $\sigma$ is a $k$-cycle, then $\varepsilon(\sigma) = (-1)^{k-1}$, i.e. $\sigma$ is odd if $k$ is even and even if $k$ is odd.

Theorem 1.4 can be rephrased by saying that the function $\varepsilon$ is well defined. The function $\varepsilon$ can be defined directly as follows:

Let $A(\sigma) \in GL_n(\mathbb{R})$ be the matrix corresponding to the linear map, also denoted $A(\sigma)$, which satisfies: for all $i$, $A(\sigma)(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$. Then $\varepsilon(\sigma) = \det A(\sigma)$.

We define $A_n$, the *alternating group*, as the kernel of $\varepsilon$, i.e.

$$A_n = \{\sigma \in S_n : \sigma \text{ is a product of an even number of transpositions}\}.$$

Thus $A_n$ is a subgroup of $S_n$. If $n \geq 2$, then $\#(A_n) = \#(S_n)/2 = n!/2$. ($A_1 = S_1$.)

# 2 Group actions

**Definition 2.1.** An *action* of the group $G$ on the set $X$ is a function $F\colon G \times X \to X$, whose value at $(g, x)$ is denoted $g \cdot x$, such that

1. For all $g, h \in G$ and $x \in X$, $g \cdot (h \cdot x) = (gh) \cdot x$.
2. For all $x \in X$, $1 \cdot x = x$.

We say $X$ is a *$G$-set*. Of course, a set $X$ may have many different interesting actions of $G$.

Given $g \in G$, define the function $L_g\colon X \to X$ by:

$$L_g(x) = g \cdot x.$$

Then $L_1 = \mathrm{Id}_X$, $L_g \circ l_h = L_{gh}$, and hence

$$L_g \circ L_{g^{-1}} = L_{g^{-1}} \circ L_g = L_1 = \mathrm{Id}_X .$$

Thus $L_g$ is a bijection (is an element of $S_X$, the group of permutations of $X$), with inverse $L_g^{-1} = L_{g^{-1}}$, and the function $g \mapsto L_g$ is a homomorphism from $G$ to $S_X$. Thus every $G$-set defines a homomorphism from $G$ to $S_X$. Conversely, if $F\colon G \to S_X$ is a homomorphism, then $F$ defines an action of $G$ on $X$ by:

$$g \cdot x = F(g)(x).$$

**Example 2.2.** The group $G$ acts on itself via: $g \cdot x = gx$. Here, the equality $g \cdot (h \cdot x) = (gh) \cdot x$ follows from the associativity of the group operation. The homomorphism $G \to S_G$ appears in the proof of Cayley's Theorem. More generally, if $H$ is a subgroup of $G$, then $G$ acts on the set of left cosets $G/H$ via the action $g \cdot (xH) = (gx)H$.

**Definition 2.3.** Given an action of $G$ on $X$, the *orbit* $G \cdot x$ of an element $x \in X$ is the set

$$\{g \cdot x : g \in G\}.$$

It is a subset of $X$. The *isotropy subgroup*

$$G_x = \{g \in G : g \cdot x = x\}.$$

It is a subgroup of $G$. For all $x \in X$, $x \in G \cdot x$, and two orbits $G \cdot x$ and $G \cdot y$ are either disjoint or equal. The action is *transitive* if there exists an $x \in X$ (equivalently, for all $x \in X$) such that $G \cdot x = X$. The orbit $G \cdot x$ is also a $G$-set, and $G \cdot x \cong G/G_x$ as $G$-sets. We define the *fixed set* $X^G$ by:

$$X^G = \{x \in X : g \cdot x = x \text{ for all } g \in G\}.$$

It is a $G$-subset of $X$.

**Example 2.4.** (1) For $G$ acting on $G$ by left multiplication, the action is transitive and the isotropy subgroup $G_g$ of any element is $\{1\}$.
(2) For $G$ acting on the left cosets $G/H$ by the action $g \cdot (xH) = (gx)H$, the action is transitive. The isotropy subgroup of $H$ is $H$, and then it is easy to check that the isotropy subgroup of $xH$ is $xHx^{-1}$. More generally, if $G$ acts on a set $X$, $x \in X$, and $y \in G \cdot x$, say $y = gx$, then the isotropy subgroups of $y$ and $x$ are related as follows: $G_y = gG_xg^{-1}$.
(3) $G$ acts on $G$ by conjugation: $i_h(g) = hgh^{-1}$. The orbit of an element $g \in G$ is the *conjugacy class* $C(g)$ *containing* $g$:

$$C(g) = \{hgh^{-1} : h \in G\}.$$

The isotropy subgroup of $g$ is the *centralizer* $Z_G(g)$ *of* $g$:

$$Z_G(g) = \{h \in G : hgh^{-1} = g\}.$$

The fixed set is the *center* $Z(G)$ *of* $G$:

$$Z(G) = \{g \in G : hgh^{-1} = g \text{ for all } h \in G\}.$$

Since $hgh^{-1} = g \iff hg = gh$, the centralizer of $g$ is the subgroup of all elements of $G$ which commute with $g$ and the center of $G$ is the subgroup of all elements of $G$ which commute with every element.