SUMMER TERM ABSTRACT ALGEBRA
HANDOUT III: CYCLIC AND DIHEDRAL GROUPS

SAMIR SIKSEK

1. Orientation

You're meant to tackle Handout III in Weeks 5 and 6. Handouts I and II aren't prerequisites. But if you haven't been through them yet, perhaps it's best to flick through them for now, and then focus on Handout III. Our aim in these handouts is to revise Term 1 Abstract Algebra and see some new examples and interesting applications.

Our academic system makes students far too dependent on academics. Lecturers, tutors and supervisors are useful, but they're not as important as they think they are. You would find life a lot more enjoyable if there were fewer contact hours and more time for independent study, and you had the opportunity to work through ideas at your own pace. This could be the term where you learn more maths than any other term, and get to enjoy it!

2. Order of an element

Definition. Let G be a group, and let $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = 1$. If there is no such positive integer, we say g has **infinite order**. In other words, g has infinite order if and only if $g^n \neq 1$ for all positive n.

In the definition, 1 is not necessarily the number 1, but the identity element in G. Also

$$g^n = \underbrace{g \circ g \circ g \circ \cdots \circ g}_{n \text{ times}}$$

where $\circ$ is the binary operation of the group G. The binary operation is not necessarily multiplication of numbers, even though we often use multiplicative notation for convenience.

If we're using additive notation, then the identity element is denoted by 0.

Definition. Let G be an additive group, and let $g \in G$. The **order** of g is the smallest positive integer n such that $ng = 0$. If there is no such positive integer, we say g has **infinite order**. In other words, g has infinite order if and only if $ng \neq 0$ for all positive n.

Date: May 18, 2020.

Exercise 1. What is the order of $g \in G$, for the following?

(i) $\rho_1 \in D_4$ (recall that ρ_1 was our notation for an anticlockwise 90° rotation around the centre of the square).
(ii) $-1 \in \mathbb{R}^*$;
(iii) $-1 \in \mathbb{R}$;
(iv) $2 \in \mathbb{R}^*$;
(v) $i \in \mathbb{C}^*$;
(vi) $\begin{pmatrix} \zeta_5 & 0 \\ 0 & \zeta_7 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ where $\zeta_m = \exp(2\pi i/m)$;
(vii) $\overline{0.75} \in \mathbb{R}/\mathbb{Z}$.
(viii) $(1,2,3)(4,5) \in S_5$.
(ix) $\overline{5}$ in $(\mathbb{Z}/7\mathbb{Z})^*$.

Exercise 2. (i) Let $A \in \mathrm{GL}_2(\mathbb{R})$. Show that if A has finite order then $\det(A) = \pm 1$.
(ii) Show that the converse of (i) is false by giving a counterexample.
(iii) Formulate the correct generalization of (i) to $A \in \mathrm{GL}_2(\mathbb{C})$.

Exercise 3. Show that

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

has infinite order in $\mathrm{GL}_2(\mathbb{R})$. **Hint.** One way of doing this is to discover a formula for A^n in terms of n. Compute A^n for the first few values of n. You should soon spot a connection to the Fibonacci sequence which you can prove by induction.

Example 1. Let's show that $\overline{\sqrt{2}}$ has infinite order in $\mathbb{R}/\mathbb{Z}$. We do this by contradiction. Suppose $\overline{\sqrt{2}}$ has finite order in $\mathbb{R}/\mathbb{Z}$. Then there is a positive integer n such that $n\overline{\sqrt{2}} = \overline{0}$, or equivalently, $\overline{n\sqrt{2}} = \overline{0}$. Recall that $\overline{a} = \overline{b}$ in $\mathbb{R}/\mathbb{Z}$ if and only if $a - b \in \mathbb{Z}$. Thus $n\sqrt{2} \in \mathbb{Z}$. Let's say that $n\sqrt{2} = m \in \mathbb{Z}$. Hence $\sqrt{2} = m/n$ (here n is positive so we can divide by it). This contradicts the fact that $\sqrt{2}$ is irrational. Hence $\overline{\sqrt{2}}$ has infinite order.

Exercise 4. Let $a \in \mathbb{R}$. Show that $\overline{a}$ has finite order in $\mathbb{R}/\mathbb{Z}$ if and only if $a \in \mathbb{Q}$.

Theorem 2. *Let $g \in G$. Suppose g has finite order n. Let $m \in \mathbb{Z}$. Then $g^m = 1$ if and only if $n \mid m$.*

Proof. The proof uses division with remainder. Have a go yourself, before reading on.

Suppose $g^m = 1$. By division with remainder, $m = qn+r$ where $0 \leq r < n$. Then

$$\begin{aligned} g^r &= g^{m-qn} \\ &= g^m \cdot (g^n)^{-q} \\ &= 1 \cdot 1^{-q} \\ &= 1. \end{aligned}$$

However n is the smallest positive integer such that $g^n = 1$ and $0 \leq r < n$. Therefore $r = 0$, and so $m = qn$. Hence $n \mid m$ as required.

The converse is easy. □

The trick using division with remainder in the above proof is used again and again throughout algebra. Make an effort to absorb it.

Theorem 3. *Let G be a finite group. Then every element $g \in G$ has finite order.*

Proof. You might say that this follows from Lagrange's theorem, which we're building up to. But this is actually a very simple result, with a very simple proof. Suppose G is finite and $g \in G$. Consider the sequence

$$g,\ g^2,\ g^3,\ g^4, \ldots .$$

This sequence looks infinite, but it has to fit inside the finite group G, so there must be repetition. Thus there are $u < v$ such that $g^u = g^v$. Hence $g^{v-u} = 1$, and $v - u$ is a positive integer. Therefore g has finite order. □

3. Cyclic Groups

Definition. Let G be a group. Let $g \in G$. We define the **cyclic subgroup generated by** g to be

$$\langle g \rangle = \{g^m \ :\ m \in \mathbb{Z}\}. \tag{1}$$

We say that G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. In this case, we say that g is a cyclic generator of G.

Of course, (1) defines $\langle g \rangle$ as a set. Calling it the 'cyclic subgroup generated by g' doesn't magically turn it into a subgroup. But you can easily check that it is indeed a subgroup of G.

Exercise 5. The above definition uses multiplicative notation. Formulate the same definition for an additive group.

Example 4. $\mathbb{Z}$ is a cyclic group, generated by 1. Note that the cyclic generator is not unique, because $\mathbb{Z}$ is also generated by -1.

Exercise 6. In D_4, compute the cyclic subgroup generated by each of the eight elements. Is D_4 cyclic?

Lemma 5. *Let G be a group, and g be an element of finite order n. Then $\langle g \rangle$ has order n. Moreover,*

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}. \tag{2}$$

Proof. Let's prove (2) first. Of course, by the definition (1), the subgroup $\langle g \rangle$ consists of all integer powers of g. Thus $\{1, g, g^2, \ldots, g^{n-1}\}$ is contained in $\langle g \rangle$. We would like to demonstrate the reverse inclusion. Suppose $h \in \langle g \rangle$. Thus $h = g^m$ for some $m \in \mathbb{Z}$. Using division with remainder, $m = qn + r$ where $0 \leq r < n$. Thus

$$\begin{aligned} h = g^m &= g^{qn+r} \\ &= (g^n)^q \cdot g^r \\ &= g^r, \end{aligned}$$

as $g^n = 1$. But $0 \leq r < n$ so $h = g^r \in \{1, g, g^2, \ldots, g^{n-1}\}$. This completes the proof of (2).

It now looks obvious that $\#\langle g \rangle = n$. However, we do have to be careful. For one thing, we haven't fully used the hypothesis that g has order n, merely that $g^n = 1$. In fact, to conclude that $\#\langle g \rangle = n$ we need to show that the list $1, g, g^2, \ldots, g^{n-1}$ does not have repetition. Suppose it does. Then there are integers u, v with $0 \leq u < v \leq n-1$ such that $g^u = g^v$. Write $m = v - u$. Then $0 < m \leq n-1$ and $g^m = 1$, contradicting the assumption that n is the order of g. □

We see again the same 'division with remainder' trick that did the work in the proof of Theorem 2.

Example 6. Let $n \geq 1$. Write $\zeta_n = \exp(2\pi i/n)$. Recall that we denoted the set of n-th roots of 1 by U_n, which we know is a subgroup of $\mathbb{C}^*$, and moreover,

$$U_n = \{z \in \mathbb{C}^* \ : \ z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} = \langle \zeta_n \rangle.$$

In particular, U_n is cyclic of order n.

Exercise 7. Which of the following groups are cyclic? Give justification. If you get stuck on a part, skip ahead, and come back when you know more about cyclic groups.

(i) $k\mathbb{Z}$ (k fixed positive integer).
(ii) $\mathbb{Z}/n\mathbb{Z}$ (n a a fixed integer ≥ 2).
(iii) S_3.
(iv) $(\mathbb{Z}/8\mathbb{Z})^*$.
(v) $\mathrm{GL}_2(\mathbb{F}_2)$.
(vi) $\mathbb{R}^2$.
(vii) $\mathbb{R}$.
(viii) $\mathbb{Q}$.

Here is a familiar fact about cyclic groups that often helps.

Lemma 7. *If G is cyclic then G is abelian.*

Proof. Suppose $G = \langle g \rangle$. Let h_1, h_2 be elements of G. Then $h_1 = g^{n_1}$, $h_2 = g^{n_2}$, so

$$h_1 h_2 = g^{n_1+n_2} = g^{n_2+n_1} = h_2 h_1.$$

Therefore G is abelian. Observe that all the proof uses is that addition of integers is commutative: $n_1 + n_2 = n_2 + n_1$. □

Example 8. Let's check that $\mathrm{GL}_2(\mathbb{F}_{13})$ is not cyclic. Recall the elements are 2×2 matrices with entries in $\mathbb{F}_{13} = \mathbb{Z}/13\mathbb{Z}$ and non-zero determinant, and the binary operation is matrix multiplication. According to the formula in Handout II,

$$\#\,\mathrm{GL}_2(\mathbb{F}_{13}) = (13^2 - 1)(13^2 - 13) = 26208.$$

The question is beginning to look scary. Do we want to try out all 26208 elements and see if they are cyclic generators? Of course not! However we can try using Lemma 7. If we can show that $\mathrm{GL}_2(\mathbb{F}_{13})$ is non-abelian, then we will know that it is non-cyclic. And to show that it is non-abelian, all we need is to find a non-commuting pair of elements. Let's take

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{13}).$$

Then

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad BA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Hence $\mathrm{GL}_2(\mathbb{F}_{13})$ is non-abelian and therefore non-cyclic. Now, we didn't use the fact that the entries live in $\mathbb{F}_{13}$. In fact, the same argument works for $\mathrm{GL}_2(K)$ for any field K.

Exercise 8. Use Lemma 7 to show that S_n is non-cyclic for all $n \geq 3$. What about S_2?

Example 9. Let's show that $\mathbb{R}^2$ is non-cyclic. This is one of those situations where it helps to think geometrically. We want to check that no $\mathbf{v} \in \mathbb{R}^2$ is a cyclic generator. Thus we want to check that for all $\mathbf{v} \in \mathbb{R}^2$,

$$\langle \mathbf{v} \rangle = \{m\mathbf{v} \ : \ m \in \mathbb{Z}\}$$

is a proper subset [1] of $\mathbb{R}^2$. Of course if $\mathbf{v} = \mathbf{0}$ then this is true, so suppose $\mathbf{v} \neq \mathbf{0}$. Write

$$L = \{\lambda \mathbf{v} \ : \ \lambda \in \mathbb{R}\}.$$

This is the subspace of $\mathbb{R}^2$ spanned by $\mathbf{v}$. It is a straight line passing through the origin. Note that

$$\langle \mathbf{v} \rangle \subset L.$$

[1] Recall that A is a **proper subset** of B if A is a subset of B but $A \neq B$. We also say B **properly contains** A.

The subspace L is a proper subspace of R^2; it is 1-dimensional and $\mathbb{R}^2$ is 2-dimensional. See Figure 1. Thus $\langle \mathbf{v} \rangle$ is a proper subset of $\mathbb{R}^2$. This is true

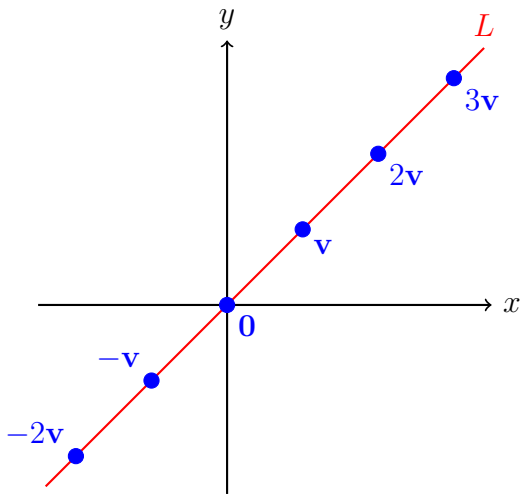

FIGURE 1. Note that $\langle \mathbf{v} \rangle$ consists of integer multiples of the vector $\mathbf{v}$. These are contained in the line L which is the span of $\mathbf{v}$, which is just the set of real multiples of $\mathbf{v}$. The subspace L is 1-dimensional (with basis element $\mathbf{v}$). It is a proper subspace of the $\mathbb{R}$-vector space $\mathbb{R}^2$ which 2-dimensional. Since L is a proper subset of $\mathbb{R}^2$ and $\langle \mathbf{v} \rangle$ is contained in L, we see that $\langle \mathbf{v} \rangle$ is properly contained in $\mathbb{R}^2$.

whatever $\mathbf{v}$ we choose. Thus $\mathbb{R}^2$ is not cyclic.

We note in passing that $\mathbb{R}^2$ is abelian but not cyclic. The converse of Lemma 7 is false.

Example 10. Let's show that $\mathbb{R}$ is non-cyclic. Let $\alpha \in \mathbb{R}$, and we want to check that

$$\langle \alpha \rangle = \{ m\alpha \ : \ m \in \mathbb{Z} \}$$

is a proper subset of R. This is true if $\alpha = 0$, so we may suppose $\alpha \neq 0$. Note that the trick we used in the previous example won't work. If we view $\mathbb{R}$ as a vector space over $\mathbb{R}$ and take the span of α then we obtain the whole of $\mathbb{R}$. Perhaps a picture here helps. See Figure 2. It is intuitively obvious that $\langle \alpha \rangle$ is not the whole of $\mathbb{R}$, but we should really specify an element of $\mathbb{R}$ that does not belong to $\langle \alpha \rangle$. Specifically, we want an element of $\mathbb{R}$ that lies in the gaps between the elements of $\langle \alpha \rangle$. Let $\beta = \alpha/2 \in \mathbb{R}$. We want to check that $\beta \notin \langle \alpha \rangle$. If $\beta \in \langle \alpha \rangle$ then $\beta = m\alpha$ with $m \in \mathbb{Z}$, so $\alpha/2 = m\alpha$ and so $m = 1/2$ (as $\alpha \neq 0$), contradicting $m \in \mathbb{Z}$. Hence $\beta \notin \langle \alpha \rangle$. Therefore $\mathbb{R} \neq \langle \alpha \rangle$ for all $\alpha \in \mathbb{R}$, so $\mathbb{R}$ is not cyclic.

Exercise 9. Show that $\mathbb{R}^*$ is non-cyclic. This is a multiplicative group, so instead of halving you want to ...?

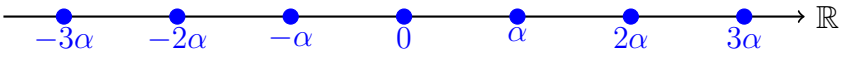

FIGURE 2. In this picture we're assuming that $\alpha > 0$. Note that $\langle\alpha\rangle$ consists of the integer multiples of α and so doesn't fill up the whole of $\mathbb{R}$.

Exercise 10. Let G be an infinite group. Suppose G has an element $h \neq 1$ of finite order. Show that G is non-cyclic.

Exercise 11. Use the result of Exercise 10 to show the following groups are non-cyclic:

(i) $\mathbb{R}^*$.
(ii) $\mathbb{C}^*$.
(iii) $\mathbb{S}$.
(iv) $\mathbb{R}/\mathbb{Z}$. This last one is additive, so you need first to translate the result of Exercise 10 to additive notation.

4. Lagrange's Theorem

Recall the three versions of Lagrange's Theorem.

Theorem 11 (Lagrange Version 1)**.** *Let G be a finite group and g an element of G. Then the order of g divides the order of G.*

Theorem 12 (Lagrange Version 2)**.** *Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G.*

Theorem 13 (Lagrange Version 3)**.** *Let G be a finite group and H a subgroup of G. Then*

$$\#G = [G : H] \cdot \#H.$$

We revisited the proof of Version 3 in Handout II. Once you have Version 3, you also have Versions 2 and 1 because of the implications

$$\text{Version 3} \implies \text{Version 2} \implies \text{Version 1}.$$

Note that the index $[G : H]$ is a positive integer; it's simply counting the number of cosets of H in G. Thus Version 3 tells us that $\#H$ is a factor of $\#G$, which is what Version 2 is saying. Also, we deduce Version 1 from Version 2 immediately by letting $H = \langle g\rangle$ and applying Lemma 5.

5. Rotations and Reflections

OK, you're bored with cyclic groups, and that's natural. They are boring. We want to move on to dihedral groups, but before that we want to revise rotations and reflections in $\mathbb{R}^2$ which you saw before in term 2 Linear Algebra. A good starting point is to observe that a rotation around the origin is a linear

transformation. More precisely, fix an angle θ, and let T_θ be anticlockwise rotation around the origin through an angle θ. Then

$$T_\theta(\mathbf{u}+\mathbf{v}) = T_\theta(\mathbf{u}) + T_\theta(\mathbf{v}), \qquad T_\theta(\alpha\mathbf{u}) = \alpha T_\theta(\mathbf{u}) \tag{3}$$

for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$ and $\alpha \in \mathbb{R}$. How do we know this? Well, we can also see this from the school definition of vector addition, and vector scaling. For that, see Figures 3 and 4. The key point is that (3) tells us that the rotation T_θ

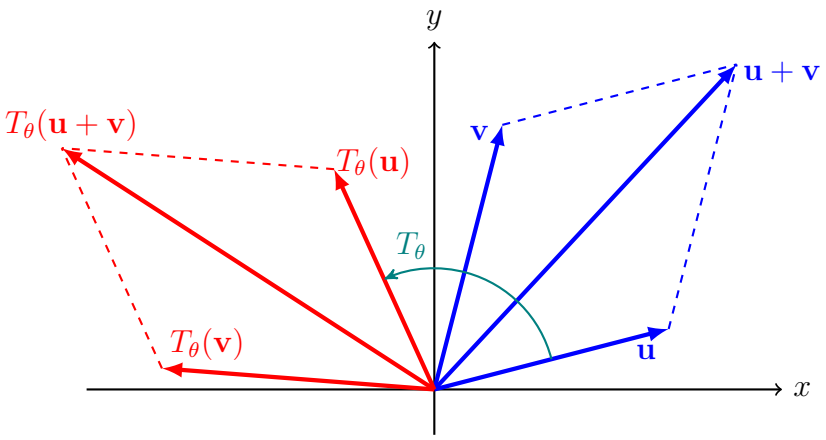

FIGURE 3. Recall how vector addition is defined geometrically. To add $\mathbf{u}$ and $\mathbf{v}$ we form the parallelogram with $\mathbf{u}$ and $\mathbf{v}$ adjacent sides starting at the origin, and then $\mathbf{u}+\mathbf{v}$ is given by the diagonal. Let T_θ be a rotation centred at the origin. Applying T_θ sends $\mathbf{u}$ to $T_\theta(\mathbf{u})$, $\mathbf{v}$ to $T_\theta(\mathbf{v})$ and $\mathbf{u}+\mathbf{v}$ to $T_\theta(\mathbf{u}+\mathbf{v})$. Crucially, $T_\theta(\mathbf{u}+\mathbf{v})$ is the diagonal of the parallelogram having $T_\theta(\mathbf{u})$ and $T_\theta(\mathbf{v})$ as adjacent sides, since a rotated parallelogram is still a parallelogram. Therefore, $T_\theta(\mathbf{u}+\mathbf{v}) = T_\theta(\mathbf{u}) + T_\theta(\mathbf{v})$, from the geometric definition of vector addition.

is a linear transformations $\mathbb{R}^2 \to \mathbb{R}^2$. We know from linear algebra (Section 8.3 of your Linear Algebra notes) that every linear transformation comes from a matrix. What does this mean? In our context it means that there is a 2×2 matrix R_θ such that $T_\theta(\mathbf{x}) = R_\theta \mathbf{x}$ (applying the rotation to the vector $\mathbf{x} \in \mathbb{R}^2$ has the same effect as multiplying the $\mathbf{x}$ by the matrix R_θ). Of course, this does not tell us how to find R_θ, but once we know it's there we can look for it.

Let $\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$, and write $T_\theta(\mathbf{x}) = \begin{pmatrix} x' \\ y' \end{pmatrix}$. We want to express x', y' in terms of x, y and θ. The easiest way to do this to use polar coordinates. Let the polar coordinates for $\mathbf{x}$ be (r, ϕ), thus

$$x = r\cos\phi, \qquad y = r\sin\phi.$$

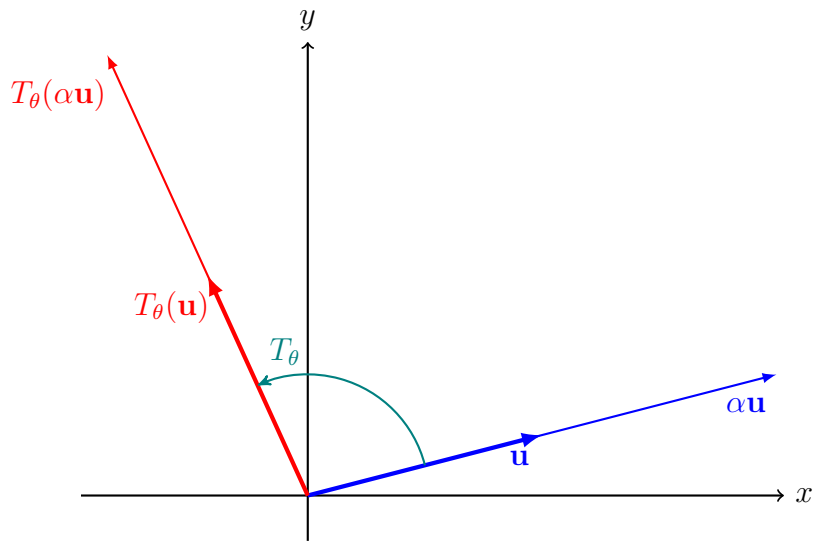

FIGURE 4. T_θ denotes a anticlockwise rotation centred at the origin through angle θ. If you scale $\mathbf{u}$ by α and then rotate you obtain $T_\theta(\alpha\mathbf{u})$. If you rotate first then scale by α you obtain $\alpha T_\theta(\mathbf{u})$. It's geometrically clear that the result should be the same either way, so we should have $T_\theta(\alpha\mathbf{u}) = \alpha T_\theta(\mathbf{u})$.

Since $T_\theta(\mathbf{x}) = \begin{pmatrix} x' \\ y' \end{pmatrix}$ is obtained by rotating $\mathbf{x}$ anticlockwise about the origin through an angle θ, it has polar coordinates $(r, \phi + \theta)$. Thus

$$x' = r\cos(\phi + \theta), \qquad y' = r\sin(\phi + \theta).$$

We expand $\cos(\phi + \theta)$ to obtain

$$\begin{aligned} x' &= r\cos(\phi + \theta) \\ &= r\cos\phi\cos\theta - r\sin\phi\sin\theta \\ &= x\cos\theta - y\sin\theta. \end{aligned}$$

Similarly

$$y' = x\sin\theta + y\cos\theta.$$

We can rewrite the two relations

$$x' = x\cos\theta - y\sin\theta, \qquad y' = x\sin\theta + y\cos\theta,$$

in matrix notation as follows

$$T_\theta(\mathbf{x}) = \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Thus anticlockwise rotation about the origin through an angle θ can be achieved by multiplying by the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Exercise 12. Check the following:

(i) $R_{\theta_1} = R_{\theta_2}$ if and only if $\theta_1 - \theta_2 \in 2\pi\mathbb{Z}$;
(ii) $R_\theta = I_2$ if and only if $\theta \in 2\pi\mathbb{Z}$;
(iii) $R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}$; why is this geometrically obvious?

Exercise 13. Write

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ : \ \theta \in \mathbb{R} \right\}.$$

(i) Check that $\mathrm{SO}_2(\mathbb{R})$ is an abelian subgroup of $\mathrm{SL}_2(\mathbb{R})$ (recall that $\mathrm{SL}_2(\mathbb{R})$ is the subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of matrices of determinant 1).
(ii) Write down some elements of finite order of $\mathrm{SO}_2(\mathbb{R})$. You might find Exercise 12 of some help.

The group $\mathrm{SO}_2(\mathbb{R})$ is called the **special orthogonal group**.

Exercise 14. In this exercise we'll do reflections. You saw how we derived the rotation matrices, and you'll follow the same steps to derive the reflection matrices. Let L_θ be a straight line through the origin which makes angle θ with the x-axis. Let $T'_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the map which sends every point to its reflection in the line L_θ.

(i) Draw pictures to convince yourself that T'_θ is a linear transformation.
(ii) Draw a picture to convince yourself that a point with polar coordinates (r, ϕ) gets sent to the point $(r, 2\theta - \phi)$ by T'_θ.
(iii) Now show that

$$T'_\theta \begin{pmatrix} x \\ y \end{pmatrix} = S_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix}, \qquad S_\theta = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}.$$

Exercise 15. Check the following:

(a) $S_\theta^2 = I_2$; why is this geometrically obvious?
(b) $R_{\theta_1} S_{\theta_2} = S_{(\theta_1/2+\theta_2)}$;
(c) $S_{\theta_1} R_{\theta_2} = S_{(\theta_1-\theta_2/2)}$;
(d) $S_{\theta_1} S_{\theta_2} = R_{2(\theta_1-\theta_2)}$.

We note the following facts

$$\text{rotation} \times \text{rotation} = \text{rotation}, \quad \text{reflection} \times \text{rotation} = \text{reflection},$$
$$\text{rotation} \times \text{reflection} = \text{reflection}, \quad \text{reflection} \times \text{reflection} = \text{rotation}.$$

Here multiplication means composition of operations. If we do a reflection and follow it up with a reflection we obtain a rotation. One fact that I found

really surprising when I first saw it is that any rotation around the origin can be obtained by composing two reflections. For example,

$$R_\theta = S_\theta S_{\theta/2}$$

which is a special case of (d) above.

Exercise 16. Let

$$\mathrm{O}_2(\mathbb{R}) = \underbrace{\{R_\theta : \theta \in \mathbb{R}\}}_{\mathrm{SO}_2(\mathbb{R})} \cup \{S_\theta : \theta \in \mathbb{R}\}.$$

(a) Show that $\mathrm{O}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.
(b) Show that $\mathrm{SO}_2(\mathbb{R})$ is a subgroup of $\mathrm{O}_2(\mathbb{R})$ of index 2.

The group $\mathrm{O}_2(\mathbb{R})$ is called the **orthogonal group**.

6. Dihedral Groups

In Introduction to Abstract Algebra we studied the group D_4 which is the group of symmetries of a square (Section V.4 of the lecture notes, and also lecture scans 2 and 3). And in the homework (specifically question B1 of Assignment 1) you studied the group D_3 which is the group of symmetries of an equilateral triangle. You might want to take a few minutes to review these before reading on.

Let $n \geq 3$. In this section we want to study the symmetries of the regular n-gon (i.e. the regular polygon with n-sides). The word regular means that all sides are equal, and all interior angles are equal. A **symmetry** of the regular n-gon is a geometric operation that leaves the n-gon occupying the same place, but might move the vertices about. The group of symmetries of the regular n-gon is denoted by D_n, and is called the **n-th dihedral group**. As you already know, D_3 is made up of 3 rotations and 3 reflections (where one of the rotations is the identity). Also D_4 is made up of 4 rotations and 4 reflections (where again one of the rotations is the identity). It seems safe to guess that D_n has order $2n$, and that it is be made up of n rotations and n reflections. This guess is correct. When we studied D_3 and D_4 we had a different symbol for each element, and we worked out a multiplication table for each of these two groups. As n grows this becomes more and more painful to do, so we will use what we learned in the previous section about rotations and reflections to help us study D_n. To get started, let's think of the regular n-gon as living in $\mathbb{R}^2$ with its centre at the origin, and with one of the vertices on the x-axis. See figure 5.

The regular n-gon has n symmetries which are rotations. These are the rotations around its centre (=origin) though angle $k \cdot 2\pi/n$ where $k = 0, 1, 2, \ldots, n-1$. Let r_k denote the rotation around the centre through angle

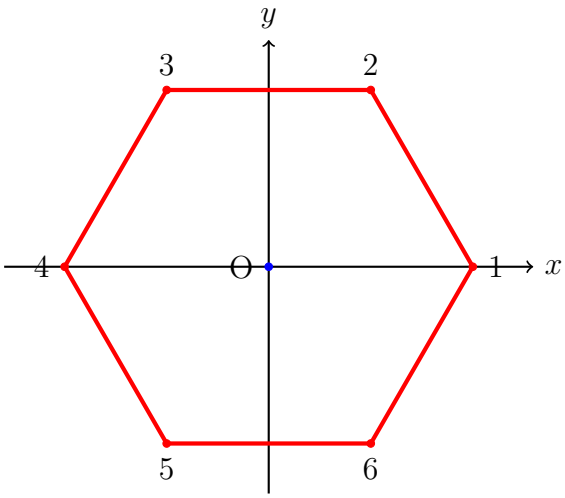

FIGURE 5. We envision the regular n-gon as being centered at the origin, with one vertex lying on the x-axis, which is labelled as 1. In this picture, $n = 6$.

$k \cdot 2\pi/n$. Then, from the previous section,

$$r_k = R_{2\pi k/n} = \begin{pmatrix} \cos 2\pi k/n & -\sin 2\pi k/n \\ \sin 2\pi k/n & \cos 2\pi k/n \end{pmatrix}.$$

Let's next talk about the symmetries of the regular n-gon which are reflections. Of course these will be reflections in certain lines passing through the origin. Recall that we used L_θ to denote the line through the origin making angle θ with the x-axis. The regular n-gon has n reflections. These are reflections in the line $L_{k\pi/n}$ for $k = 0, 1, 2, \ldots, n-1$. Just draw pictures with $n = 3$, 4, 5, 6 to convince yourself that this is true (and remember to position the n-gon with the centre at the origin and a vertex on the x-axis!). Let's write

$$s_k = S_{\pi k/n} = \begin{pmatrix} \cos 2\pi k/n & \sin 2\pi k/n \\ \sin 2\pi k/n & -\cos 2\pi k/n \end{pmatrix}$$

for the reflection in the line $L_{k\pi/n}$. Thus

$$D_n = \underbrace{\{r_0, r_1, \ldots, r_{n-1}\}}_{\text{rotations}} \cup \underbrace{\{s_0, s_1, \ldots, s_{n-1}\}}_{\text{reflections}}.$$

We can of course multiply the elements of D_n using the formulae in Exercises 12 and 15. But we can simplify things even further. Instead of working with $2n$ symbols akwardly denoted $r_0, \ldots, r_{n-1}$ and $s_0, \ldots, s_{n-1}$, we can write

all elements in terms of just two which we denote by r and s. Let

$$r = r_1 = R_{2\pi/n} = \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{pmatrix},$$
$$s = s_0 = S_0 = \begin{pmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Note that r is simply anticlockwise rotation around the origin through an angle of $2\pi/n$, and s is reflection in the x-axis (the line L_0).

Exercise 17. Check the following,

(a) $r_k = r^k$,
(b) $s_k = r^k \cdot s$,
(c) r has order n,
(d) s has order 2,
(e) $sr = r^{-1}s = r^{n-1}s$.

It follows that we can write

$$D_n = \{\underbrace{1, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}\} \cup \{\underbrace{s, rs, r^2s, \ldots, r^{n-1}s}_{\text{reflections}}\}. \tag{4}$$

The elements r, s are **generators** of D_n. We can write every element of D_n in terms of r, s. Let's talk about how to multiply the elements of D_n once we've represented them as in (4). Of course, it's easy to multiply the rotations:

$$r^k \cdot r^\ell = r^{k+\ell}.$$

But there is a subtlety. The exponent of r only matters modulo n, as r has order n. This mean that we compute $k + \ell$ and then take its remainder modulo n. What about multiplying a rotation with a reflection? A rotation has the form r^k for some $0 \leq k \leq n-1$ and a reflection has the form $r^\ell s$ for some $0 \leq \ell \leq n-1$. If we wanted to multiply $r^\ell s \cdot r^k$ then we need to think a little. We want the answer to belong to the list of reflections in (4). This means that somehow the answer should have the form $r^u s$. Note that s should be on the right. In the expression $r^\ell s \cdot r^k$, the s is in the middle. We want to shift it to the right. We will make use of the identity $sr = r^{-1}s$

from Exercise 17. Note that

$$\begin{aligned} r^\ell s \cdot r^k &= r^\ell \cdot sr \cdot r^{k-1} \\ &= r^\ell \cdot r^{-1} s \cdot r^{k-1} && \text{using } sr = r^{-1}s \\ &= r^{\ell-1} \cdot s \cdot r^{k-1} \\ &= r^{\ell-1} \cdot sr \cdot r^{k-2} \\ &= r^{\ell-1} \cdot r^{-1} s \cdot r^{k-2} \\ &= r^{\ell-2} \cdot s \cdot r^{k-2} \\ &= r^{\ell-3} \cdot s \cdot r^{k-3} && \text{repeat the above steps} \\ &= \cdots = r^{\ell-k} \cdot s \cdot r^0 = r^{\ell-k} s. \end{aligned}$$

Of course the exponent $\ell - k$ is reduced modulo n.

Exercise 18. Complete the following table of multiplication rules for D_n:

	r^k	$r^k s$
r^ℓ	$r^{\ell+k}$	
$r^\ell s$	$r^{\ell-k} s$	

Exercise 19. (Optional) A certain group G of order 20 is generated by two elements x, y where x has order 4, y has order 5 and moreover, $xy = y^2 x$. It can be shown (you're not asked to do this) that every element can be written uniquely as $y^b x^a$ where $b \in \{0, 1, 2, 3, 4\}$ and $a \in \{0, 1, 2, 3\}$. Complete the following table of multiplication rules for G:

	y^k	$y^k x$	$y^k x^2$	$y^k x^3$
y^ℓ				
$y^\ell x$				
$y^\ell x^2$				
$y^\ell x^3$				

Hint: show first that $xy^b = y^{2b} x$.