Visual Algebra

Lecture 2.2: Cyclic groups

Dr. Matthew Macauley

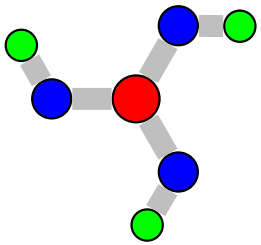
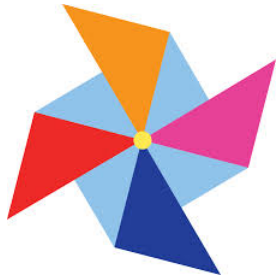
School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Cyclic groups

Definition

A group is cyclic if it can be generated by a single element.

Finite cyclic groups describe the symmetries of objects that have *only* rotational symmetry.


We have seen three ways to represent cyclic groups.

1. By roots of unity:

$$C_n \cong \langle \zeta_n \rangle = \langle e^{2\pi i/n} \rangle = \left\{ e^{2\pi ik/n} \mid k = 0, \ldots n-1 \right\} \subseteq \mathbb{C}.$$

2. By real rotation matrices:

$$C_n \cong \langle A_{2\pi/n} \rangle = \left\langle \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \right\rangle.$$

3. By complex rotation matrices:

$$C_n \cong \langle R_n \rangle = \left\langle \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix} \right\rangle.$$

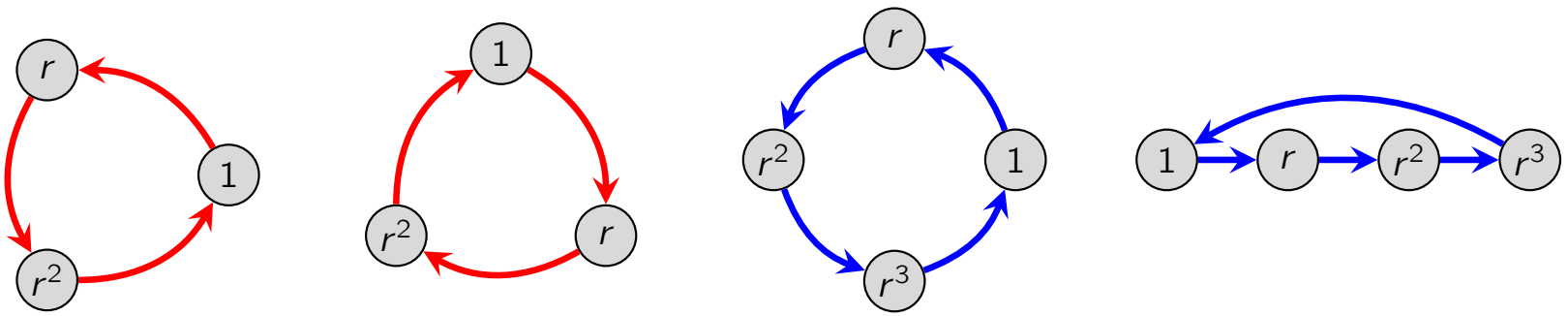
Cyclic groups, multiplicatively

Definition

For $n \geq 1$, the multiplicative cyclic group C_n is the set

$$C_n = \{1, r, r^2, \ldots, r^{n-1}\},$$

where $r^i r^j = r^{i+j}$, and the exponents are taken modulo n. The identity is $r^0 = r^n = 1$.



It is clear that a presentation for this is

$$C_n = \langle r \mid r^n = 1 \rangle.$$

Note that r^2 generates C_5:

$$(r^2)^0 = 1, \quad (r^2)^1 = r^2, \quad (r^2)^2 = r^4, \quad (r^2)^3 = r^6 = r, \quad (r^2)^4 = r^8 = r^3.$$

Do you have a conjecture about for which k does $C_n = \langle r^k \rangle$?

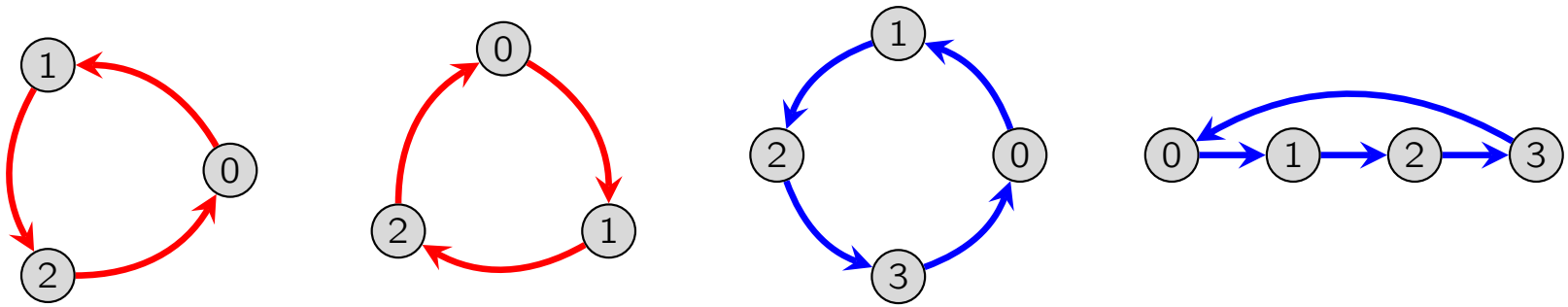
Cyclic groups, additively

Definition

For $n \geq 1$, the additive cyclic group $\mathbb{Z}_n$ is the set

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

where the binary operation is addition modulo n. The identity is 0.



We can write a group presentation additvely:

$$\mathbb{Z}_n = \langle 1 \mid n \cdot 1 = 0 \rangle.$$

Note that 2 generates $\mathbb{Z}_5$:

$$0 \cdot 2 = 0, \qquad 1 \cdot 2 = 2, \qquad 2 \cdot 2 = 4, \qquad 2 \cdot 3 = 6 \equiv_5 1, \qquad 2 \cdot 4 = 8 \equiv_5 3.$$

Remark

It is wrong to write $C_n = \mathbb{Z}_n$; instead, we say $C_n \cong \mathbb{Z}_n$.

Generators of cyclic groups

Recall that the greatest common divisor of nonzero $a, b \in \mathbb{Z}$ is

$$\gcd(a, b) = \min\left\{|ax + by| : x, y \in \mathbb{Z}\right\},$$

and they are co-prime if $\gcd(a, b) = 1$.

Proposition

A number $k \in \{0, 1, \ldots, n-1\}$ generates $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

Equivalently, $C_n = \langle \zeta_n^k \rangle$ if and only if $\zeta_n^k = e^{2\pi ik/n}$ is a primitive n^{th} root of unity.

Proof

"$\Leftarrow$": We need to show that $1 \in \langle k \rangle$.

In other words, that $1 \equiv_n ky$ for some $y \in \mathbb{Z}$.

If $\gcd(n, k) = 1$, then write $1 = nx + ky$ for some $x, y \in \mathbb{Z}$. Taking this modulo n yields

$$1 \equiv_n nx + ky \equiv_n ky.$$

We'll leave the "$\Rightarrow$" direction as an exercise. □

Cayley tables of cyclic groups

Modular addition has a nice visual appearance in the Cayley tables for cyclic groups, if we order the elements $0, 1, \ldots, n-1$.

Here are two different ways to write the Cayley table for $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

	0	1	3	2	4
0	0	1	3	2	4
1	1	2	4	3	0
3	3	4	1	0	2
2	2	3	0	4	1
4	4	0	2	1	3

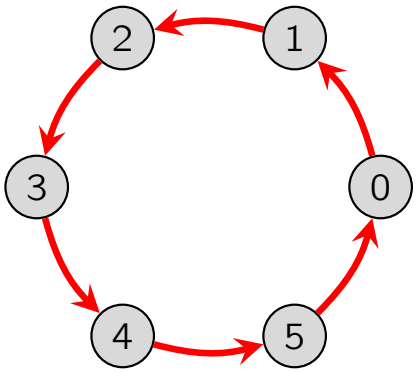
The second Cayley table was one of our mystery Latin squares from the previous chapter.

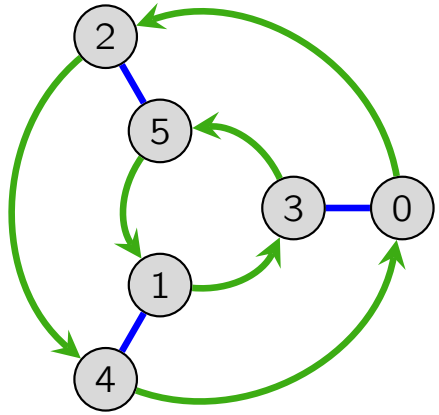
Minimal vs. minimum generating sets

There are many ways to generate the cyclic group of order 6:

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle = \langle 2, 3 \rangle = \langle 3, 4 \rangle = \langle 1, 2 \rangle = \langle 1, 2, 3 \rangle = \cdots$$

The following Cayley graphs illustrate two of these.





Definition

Given $G = \langle S \rangle$, the set S is a minimal generating set if $T \subsetneq S$ implies $\langle T \rangle \neq G$.

It is minimum if it is minimal, and $|S| \leq |T|$, for all other min'l generating sets T.

Finite groups always have at least one minimum generating set.

What about infinite groups?

Infinite cyclic groups

Definition

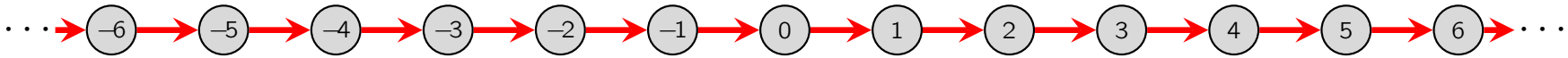
The additive infinite cyclic group is

$$\mathbb{Z} = \langle 1 \mid \quad \rangle,$$

the integers under addition. The multiplicative infinite cyclic group is

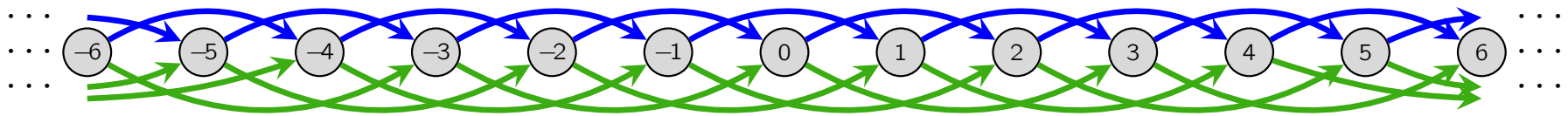
$$C_\infty := \langle r \mid \quad \rangle = \{r^k \mid k \in \mathbb{Z}\}.$$

Several of our frieze groups were cyclic.



There are only two choices for a minimum generating set: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

There are many choices for larger minimal generating sets. Here is $\mathbb{Z} = \langle 2, 3 \rangle$:



Orbits and cycle graphs

Definition

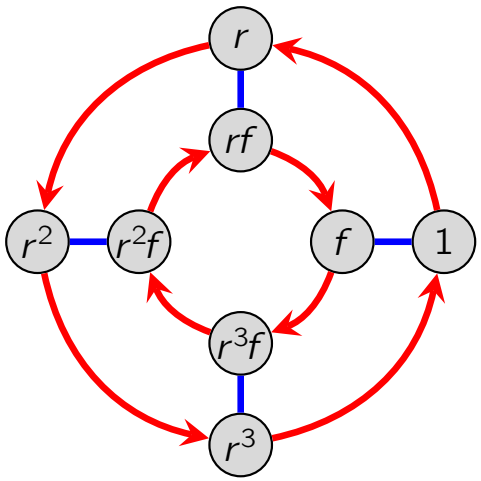
The orbit of an element $g \in G$ is the cyclic subgroup

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \},$$

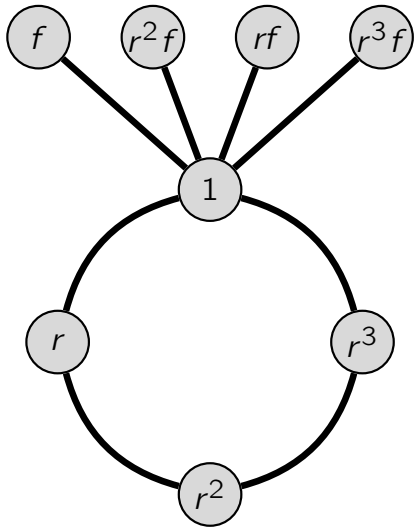
and its order is $|g| := |\langle g \rangle|$.

We can visualize the orbits by the (undirected) orbit graph, or cycle graph.

This is best seen by an example:



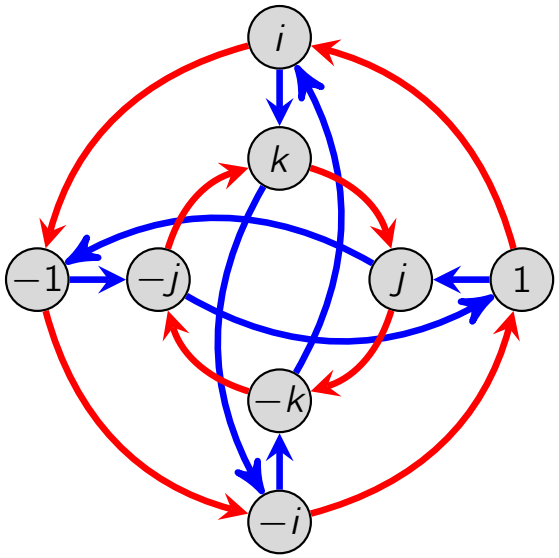
element	orbit
1	$\{1\}$
r^2	$\{1, r^2\}$
r r^3	$\{1, r, r^2, r^3\}$
f	$\{1, f\}$
rf	$\{1, rf\}$
$r^2 f$	$\{1, r^2 f\}$
$r^3 f$	$\{1, r^3 f\}$



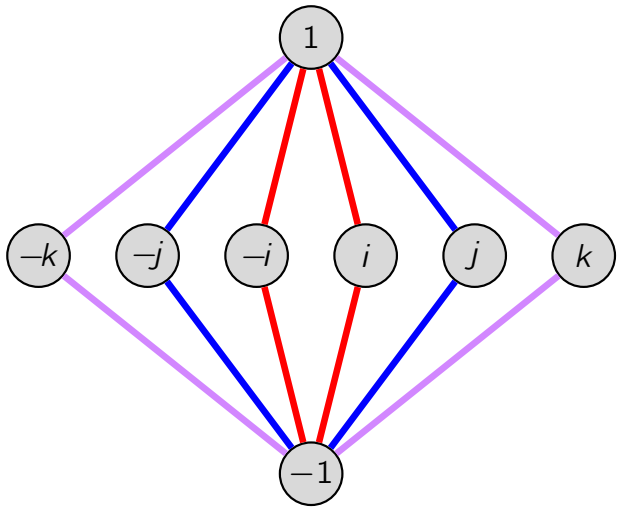
By convention, we typically only draw maximal orbits.

Orbits and cycle graphs

Here is a cycle graph for the quaternion group $Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$.



element	orbit
1	$\{1\}$
-1	$\{\pm 1\}$
i $-i$	$\{\pm 1, \pm i\}$
j $-j$	$\{\pm 1, \pm j\}$
k $-k$	$\{\pm 1, \pm k\}$



Remarks

- We colored the edges to eliminate ambiguity. This is optional, but often helpful.
- We left the edges undirected, because doing so does not introduce ambiguity.
- All of the maximal orbits have size 4.
- All of the size-4 orbits intersect in a size-2 orbit, $\{1, -1\}$.