Yi Liaw

19239969

MA3343: Groups (Poster Project)

7. The number of generators of a cyclic group

We will first prove the general fact that all elements of order k in a cyclic group of order n, where k and n are relatively prime, generate the group. This implies that if n is prime, the $n-1$ elements other than the identity generate the group.

First, notice that elements of the form x^p where p and n are not relatively prime cannot generate the group.

To see this, let

$$p = ak, n = bk$$

where $a < b$ and $1 < k \in \mathbf{Z}$. Then the largest possible order of x^p would be b, since

$$x^{pb} = x^{bak} = (x^{bk})^a = (x^n)^a = 1^a = 1.$$

However, $b < n = bk$, so the order of $x^p < n$, so x^p cannot be a generator.

Now notice that an element of the form x^q where q and n are relatively prime has order n.

To see this, note that we only have to show that x^q has order at least n, since it clearly has order at most n. Assume x^q is of order j, where $j < n$. Then

$(x^q)^j = x^{qj}$ implying that $qj = ln$ for some $l \in \mathbf{Z}$.

However, since n doesn't divide q, n must divide j, which is impossible since $j < n$.

Therefore, x^q has order n, and its n powers are distinct, so x^q must generate the group.

Now we can easily see that in a cyclic group of order 5, x, x^2, x^3, and x^4 generate this group.

In a cyclic group of order 6, x and x^5 generate the group.

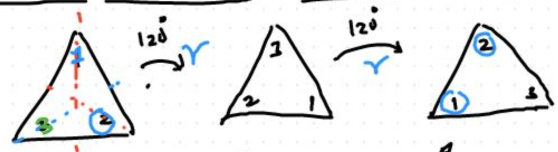
In a cyclic group of order 8, x, x^3, x^5, and x^7 generate the group.

In a cyclic group of order 10, x, x^3, x^7, and x^9 generate the group.

NON ABELIAN GROUP WITH ABELIAN SUBGROUP

$r = 120°$

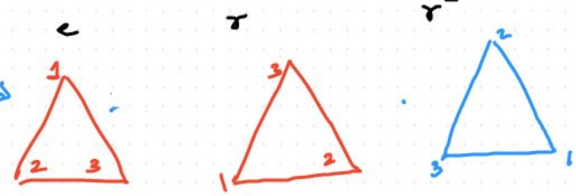
Array notation



e	R_{120}	R_{240}
e	r	r^2

$e \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

e	$(1\,2\,3)$	$(1\,3\,2)$
e	r	r^2



f	$r^2 f$	rf

r

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$(2\,3)$	$(1\,3)$	$(1\,2)$
f	$r^2 f$	rf

$(1\,3\,2)(1\,3\,2) = (1\,2\,3)$

$(1\,2\,3)(1\,3\,2) = e \mid (1\,3\,2)(1\,2\,3) = e$

$(1\,2\,3)(1\,2\,3) = (1\,3\,2)$

then / after

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \to \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} \to \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$

right →

left ↓

	e	$(1\,2\,3)$	$(1\,3\,2)$
e	e	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	e
$(1\,3\,2)$	$(1\,3\,2)$	e	$(1\,2\,3)$