The Number of Generators of a Cyclic Group

Remus Ariton Emmet Connolly Cathal Byrne

MA3343

Cyclic Groups

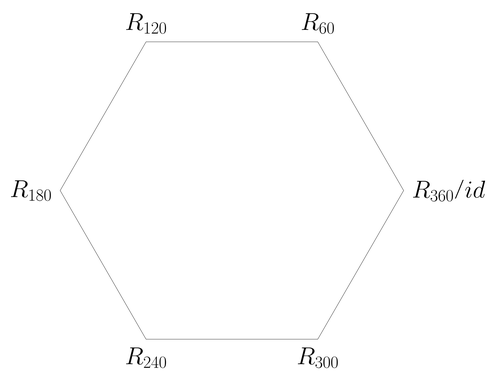

Figure 1:Rotational symmetries of D_{12}.

Let G be a group with operation $*$.
G is a cyclic group if all elements of G can be generated by a single element a and a^{-1}, where $a \in G$.
i.e G is cyclic if $G =< a >$ for some $a \in G$.
Cyclic subgroups may have more than one generating element a.

Cyclic Subgroups

A cyclic subgroup of a group can be generated by taking $x \in G$ and combining it with itself and x^{-1} to assemble a sequence of elements.

$$\ldots\ x^{-1} * x^{-1} * x^{-1},\ x^{-1} * x^{-1},\ x^{-1}, id, x, x * x,\ x * x * x \ldots$$

- A cyclic subgroup also happens to be the smallest subgroup to contain x.
- Example of a cyclic subgroup of $\mathbb{Z}$: $9\mathbb{Z}$ under the addition operator.

$$\ldots\ -36, -27, -18, -9, 0, 9, 18, 27, 36 \ldots$$

- Example of a subgroup of the dihedral group D_{12} :The rotational symmetries of D_{12} (D_{2n} where n=6 polygon). figure 1
  The group consisting of rotations by $\frac{n2\pi}{6}$ for $n = \{1, 2, \ldots, 6\}$ in the anticlockwise direction.
  The rotation $\frac{2\pi}{6}$ is an immediate example of generating element of this subgroup.

Finite Cyclic Group C_n

Elements of C_n (cyclic group with n elements) can be represented as such

$$\{x, x^2, \ldots x^n\},\ id = x^n$$

The exponent of x^{n} n indicates that x^{n} has been generated by applying x under the operation $*$ by itself $n-1$ times. e.g

$$x^3 = x * x * x$$

Generating elements of C_n from elements of C_n can be achieved by multiplication under modulus n.

$$x^i \cdot x^j = x^{(i+j)/n}$$

Where $(i+j)/n$ denotes the remainder on dividing i + j by n.
This enables us to understand which elements of C_n are generating elements of the cyclic group.

Generating Elements

Lets choose x^i as a candidate to be a generating elelment ofC_n.
Applying x^i to itself under the group operation creates elements $x^{\frac{im}{n}}$ where $m \in \mathbb{Z}$
For $x^i$to be a generating element $\frac{im}{n}$ must create the set $\{1, 2, \ldots n\}$ relating to each $x^i \in C_n$
If $x^i \in C_n$ is to generate C_n as a cyclic group i and n must be coprime in order for all elements to be produced.
Example of coprimes: 7 and 9 as they only share the factor 1.

- E.x:cyclic group $9\mathbb{Z}$ = $\{0, 1, 2, 3, \ldots, 8\}$.
  let $x^i = 2$ as 2 is coprime with 9

$$(2\cdot 0/)9 = 0, (2\cdot 1)/9 = 2, (2\cdot 2)/9 = 4, (2\cdot 3)/9 = 6, (2\cdot 4)/9 = 8, (2\cdot 5)/9 = 1$$
$$(2\cdot 6)/9 = 3, (2\cdot 7)/9 = 5, (2\cdot 8)/9 = 7,$$
$$< 2 >= \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = 9\mathbb{Z}$$

- E.x: Rotational symmetries of D_{12} = $\{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$ id=R_{360}.
  let $x^i = x^5 = R_{300}$, clear that 5 is coprime to 6.

$*$	id	R_{300}	R^2_{300}	R^3_{300}	R^4_{300}	R^5_{300}
R_{300}	R_{300}	R_{240}	R_{180}	R_{120}	R_{60}	id

$$< R_{300} >= \{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$$

If i and n are not coprime, $(i \cdot m)/n$ where $m \in \mathbb{Z}$ will cycle through a set containing some but not all elements of $\{1, 2, \ldots, n\}$ relating to each $x^i \in C_n$. Such x^i fail to generate all elements of C_n.

Generating Sets

x^j is an element which will generate C_n as a cyclic group, as j and n are coprime.
The order of the set of all such elements is simply Euler's totient function ϕ of n ie(the order of the set of numbers $< n$ which are co prime to n).

$$e.g : \phi(9) = |a|,\ where\ a\ is\ the\ set\ \{1, 2, 4, 5, 7, 8\}$$
$$\phi(9) = 6$$

- The generating set of the group of rotational symmetries of D_{12}.
  Order of R = $\{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$ is 6.

$$\phi(6) = |r|,\ where\ r\ is\ the\ generating\ set\ \{R_{60}, R_{300}\}$$
$$\phi(6) = 2$$

Infinite Cyclic Group

Let $< g >$ = G be an infinite cyclic group. For any infinite cyclic group G there are 2 generators. These generators are g^{-1} and g. .

Proof

If G = $< g >$ and G = $< h >$
Then g = h^n for some integer n and h = g^{mn}
G is infinitely cyclic so mn = 1
m and n are integers so they can only satisfy mn = 1 if m =1 and n=1 or (m = -1 and n = -1)
Therefore n = 1 or n = -1
Thus the only possible generators are g and g^{-1}

References

Cyclic Groups (Abstract Algebra) (2016) YouTube video, added by Socratica [Online]. Available at https://www.google.com/url?sa=tsource=webrct=jurl=https://m.youtube.com/watch%3Fv%3D8A84sA1YuPwved=2ahUKEwjKmInyvM7tAhUDqXEKHSNyCT0Qt9IBMA56BAgSEAgusg=AOvVaw2de3NB3FcXNAvyGYfmF151 [Accessed 14th of December 2020]

Unit, "An Infinite Cyclic Group has Exactly Two Generators: Is My Proof Correct?. [Accessed 13th of December 2020] https://math.stackexchange.com/questions/1075889/an-infinite-cyclic-group-has-exactly-two-generators-is-my-proof-correct ," (2014).