Today: ① More conjugation stuff
② Cyclic groups

Quiz

1. Let G be a group and $a \in G$.
   (i) What is the order of G?
   (ii) What is the order of a?

2. Let $C_n = \langle a : a^n = 1 \rangle$ be a cyclic group, and let $k \in \mathbb{Z}_{>0}$.
   Give an expression for the order of a^k in terms of n and k.

Conjugacy

Let G be a group

$a, b \in G$ are conjugate if $\exists\, c \in G$ s.t. $a = cbc^{-1}$.

$H_1, H_2 < G$ are conjugate if $\exists\, c \in G$ s.t. $H_1 = cH_2c^{-1}$

Conjugacy forms an equivalence relation for both elements and subgroups.

Examples

* In S_4, (132) and $(1234)(132)(1234)$ are conjugate.

  ($(1234)(132)(1432) = (1234)(1423) = (243)$)

* The subgroup $(1234)\langle(132)\rangle(1234)^{-1}$ is the subgroup $\langle(243)\rangle$

  Aside: If $H < G$ is generated by $h_1, \ldots, h_k$, then cHc^{-1} is generated by $ch_1c^{-1}, \ldots, ch_kc^{-1}$. For example, $ch_1h_4h_3c^{-1} = (ch_1c^{-1})(ch_4c^{-1})(ch_3c^{-1})$.

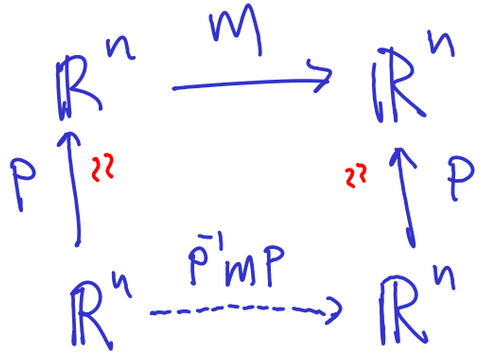
  Aside 2 If $a \in G$, then $a^n = 1 \Leftrightarrow (cac^{-1})^n = 1$. So a and cac^{-1} have the same order.

  $(cac^{-1})^n = (cac^{-1})(cac^{-1})(cac^{-1})\cdots(cac^{-1}) = ca^nc^{-1}$

* In an abelian group, the equivalence class of each element and of each subgroup contains only a single element. [$cac^{-1} = acc^{-1} = a$].

* What does conjugation mean in $GL_n(\mathbb{R})$? Answer: Change of basis.

Let $M, P \in GL_n(\mathbb{R})$. Then we have linear transformations:



Big Picture

In general, if G is a group and $a \in G$, conjugation gives a bijection

$$G \longrightarrow G$$
$$g \longmapsto aga^{-1}$$

permuting the elements of G and the subgroups of G.

Cyclic Groups

Let C_n be the group generated by a single element of order n; $C_n = \langle a \rangle$ with $|a| = n$

Main results

1. $a^i = a^j$ iff $i = j \bmod n$.
2. a^k generates C_n iff $\gcd(k,n) = 1$. In general, $|a^k| = \frac{n}{\gcd(k,n)}$.
3. Each subgroup of C_n is cyclic and its order divides n.
4. For each k dividing n, there is exactly one subgroup of order k: $\langle a^{n/k} \rangle$.
5. The number of subgroups of C_n is the number of divisors of n.

Def (Euler ϕ-function) For $n \in \mathbb{Z}_{>0}$

$$\phi(n) = \left| \{ k \in \mathbb{N} : 1 \le k < n \text{ and } \underbrace{k \text{ relatively prime to } n}_{\gcd(k,n)=1} \} \right|.$$

Thm.

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \qquad \text{[product over primes } p \text{ dividing } n\text{]}$$

Example $C_{12} = \{1, a, a^2, \ldots, a^{11}\}$, $a^{12} = 1$

elt.	1	a	a^2	a^3	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
order	1	12	6	4	12	2	12	3	4	6	12

↖ E.g., $\gcd(8,12) = 4$, and $\frac{12}{4} = 3 = \text{order}(a^8)$.

Sage examples:

① # of subgroups of C_n as n varies

② # of different generators of C_n

Two key ideas behind structure of cyclic groups

Division Algorithm If $m, n \in \mathbb{Z}$, $n > 0$, $\exists\, q, r$ s.t.

$$m = qn + r, \quad 0 \le r < q$$

q: quotient; r: remainder

Euclidean Algorithm For $m, n \in \mathbb{Z}_{>0}$, you can calculate $\gcd(m,n)$ as follows: Say $m > n$. Let $m' = m \bmod n$. If $m' = 0$, then $\gcd(m,n) = n$. Otherwise replace (m,n) by (m',n). Now $m' < n$. Let $n' = n \bmod m'$. If $n' = 0$, then $\gcd(m,n) = m'$. Otherwise, replace (m', n) by (m', n'). Now $n' < m'$. Continue.

Example $(81,57) \to (24,57) \to (24,9) \to (6,9) \to (6,3) \to (0,3)$

$\gcd(81,57) = 3$.

Proof of some of the main results

* If $a^k = e$, then k is a multiple of $|a|$.

Pf/ Use the division algorithm to write $k = q|a| + r$, $0 \le r < |a|$.

Then $e = a^k = a^{q|a|+r} = a^{q|a|} a^r = e \cdot a^r = a^r$. Since $r < |a|$, by definition of $|a|$, we must have $r = 0$. Thus, $k = q|a|$. □