MATH 335 lecture 16

Chris Camano: ccamano@sfsu.edu

October 24, 2022

$$V_+ = \begin{pmatrix} \sigma_x^2 + \sigma_{xy} - \lambda_- \\ \sigma_y^2 + \sigma_{xy} - \lambda_- \end{pmatrix} \quad V_- = \begin{pmatrix} \sigma_x^2 + \sigma_{xy} - \lambda_+ \\ \sigma_y^2 + \sigma_{xy} - \lambda_+ \end{pmatrix}$$

Theorem 1. : Let G be a group, and a$\in G$ if the order of a is n, this is to say :

$$|a| = n \rightarrow |a^k| = \frac{n}{\gcd(k,n)}$$

$$\forall n \in \mathbb{Z}, \gcd(k,n)|n \therefore \gcd(k,n)|n$$

Proof. Let d=gcd(k,m) for brevity:
This implies that $d|k, d|m$ which implies: $k = db, n = dc$
b and c have a gcd equal to one since d is the greatest common divisor of n and k.

Let y=a^k (the element whose order we are interested in identifying)

Observe that: $y^{\frac{n}{d}}$ is the identity.

$$y^{\frac{n}{d}} = (a^k)^{\frac{n}{d}} = (a^d b)^{\frac{n}{d}} = (a^{bn}) = (a^n)^b = (e)^b = e$$

According to the lemma below the order of y must divide $\frac{n}{d} = c$. in other words:

$$|a^k||c \rightarrow n|c$$

$$(a^k)^{|a^k|} = e = a^{k|a^k|}$$

so

$$n|(k|a^k|) \rightarrow dc|(db|a^k|) \rightarrow c|b(|a^k|)$$

This implies that c divides $|a^k|$ since $gcd(c,b) = 1$

This combined with teeh fact that $|a^k||\frac{n}{d}$ we arrive to our conclusion that

$$|a^k| = \frac{n}{d} = \frac{|a|}{\gcd(k,n)}$$

□

Lemma

: Let G be a group, and $a \in G$ let $|a| = m$ then a^t is the identity iff $m|t$. This is to say the only way to get the identity element is to raise the element to a ultiple of its order which follows from the fact that under the modular operation of the identity the only way to return to zero is by multiplying by multiples of the identity.

Proof. The first direction of the proof is the following:

$$a^m = e, t = ms, s \in \mathbb{Z}$$

and we want to show that:

$$a^t = e$$

this is equivilant tos aying :

$$a^t = a^{mk} = (a^m)^s = (e)^s$$

The other direction of the proof is as follows: Given:

$$a^t = e$$

show that t=ms$s \in \mathbb{Z} \to m|t$ By division algorithm

$$\begin{aligned} &t = qm + r, 0 \leq r < m \\ &a^t = e \to e = a^t = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = (e^q)a^r = ea^r = a^r \end{aligned}$$

but r is less than m and the first time we arrive to the identity is when a is equal to m. this implies that r must be equal to zero □

corollary

If G is a cyclic group where the element has order n, this is to say:

$$G =< a > \{e, a, a^2, ..., a^{n-1}\}$$

Then $< a^k >$ is a cyclic subgroup with $\frac{n}{\gcd n,k}$ elements

Proof.

$$< a^k >= \{e,^k, a^{2k}, ..., a^{\frac{n}{\gcd k,n}-1}\}$$

all powers of a generator that are relativley prime to the order of the generator are equal to the group .
Formalization:

□

f $G =< a >$ where $|a| = n$ then $G =< a^k >$ iff and only if gcd(k,n)=1 meaning that a cyclic group of order n has $\phi(n)$ generators. Cyclic groups of prime order have the property that every no identity element is a generator.
The order of a group is the cardinality of the group.