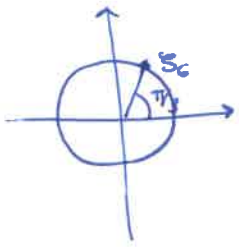
W3 summary (an example)



Consider $\zeta_6 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$

ζ_6 is a 6-th root of unity
(a complex number whose 6-th power is 1)

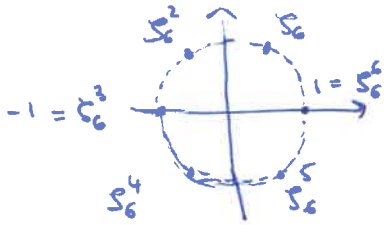
$\zeta_6 \in (\mathbb{C}^\times, \cdot)$ (in fact, it belongs to the subgroup from problem 7(d))

$\langle \zeta_6 \rangle = \{1, \zeta_6, \zeta_6^2, .. \zeta_6^5\}$

↑ subgroup generated by all integral powers of ζ_6.
There exist a unique (smallest positive exponent for which the integral power of the element gives the identity (here: $1 \in \mathbb{C}^\times$)
In this case 6 is this integer. We call this number the order of the element.

$o(\zeta_6) = 6$ and $6 = |\langle \zeta_6 \rangle|$

Visually:



the 6 elements of the cyclic subgroup $\langle \zeta_6 \rangle \leq \mathbb{C}^\times$ are the vertices of a regular hexagon on the unit circle.

These features of cyclic subgroups generated by an element $g \in G$: $g^t = e \Leftrightarrow t$ is a multiple of $o(g)$

There $\exists$ { finite (like $\langle \zeta_6 \rangle$) / infinite } cyclic groups.

For instance $\langle 2 \rangle \leq \mathbb{Z}$ is ∞

Can you identify subgroups of $\langle \zeta_6 \rangle$? We'll see today that subgroups of cyclic groups are very well understood.

Lecture 7

1.7 Groups: Order of subgroups & Lagrange's theorem.

In our analysis of the subgroup structure of S_4, we noticed that there seems to be a relationship between the order of subgroups and that of the group.

$|S_4| = 4! = 24$ and we found subgroups of order 2, 3, 4, 6, 8, 12 (and trivially 1 and 24).

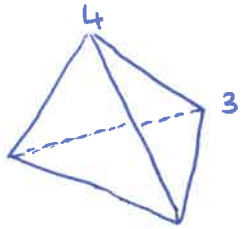
These are exactly the divisors of 24.

Ideas: $\not\rightarrow$ there is (at least) a subgroup of order k for all k divisors of the order of the gp

and/or $\rightarrow$ if $H \leq G$ then its order divides that of G.

The first <u>does not hold</u> in general:

Example $A_4 = \{\text{even permutations of } S_4\}$ has order 12. We can visualise this group as the group of symmetries of a regular tetrahedron



Elements of this gp are: e, 8 three-cycles of S_4 (corresponding essentially to fixing a vertex of the tetrahedron and rotating the opposite face), and the three double transpositions: $(12)(34)$, $(13)(24)$, $(14)(23)$.

You can check that A_4 has subgroups of order 2, 3, 4 but not 6.

The second of our observations/ideas holds true for all finite groups. It is known as Lagrange's theorem for finite groups.

Thm (Lagrange) If G is a finite group and $H \leq G$ then the <u>order of H divides the order of G</u>.

Rmk Lagrange's thm simplifies the problem of finding subgroups of a finite group, in the sense that it greatly restricts the possible orders which subgroups can have. It doesn't, on the other hand, tell us anything on whether for a certain divisor of the order we will find or not a subgroup of that order.

Note that Lagrange's thm can be re-stated for order of elts: $|G|<\infty, g \in G \Rightarrow o(g) \mid |G|$

There are two results in the other direction which help identifying/determine the existence of subgroups of prescribed order: a "structure theorem" for finite cyclic groups, and Cauchy's theorem on subgroups of prime order. We will start with the first, after having introduced a new (not so new to you, in fact) family of finite abelian groups.

Example/Definition Let $n \in \mathbb{N}$. Define $\mathbb{Z}_n$ to be the set of "integers modulo n"

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Define an operation $+_n$ (we will simply write $+$): $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ as follows

$$a+b = \begin{cases} a+b, & \text{if } a+b \leq n-1 \\ a+b-n, & \text{if } a+b \geq n \end{cases}$$

<u>Facts</u>

- $(\mathbb{Z}_n, +)$ is an abelian group of order n.
- $(\mathbb{Z}_n, +) = \langle 1 \rangle$ $\forall n$, that is $\mathbb{Z}_n$ is a cyclic gp generated by 1.

Example $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$

here $3+6=1$

and $2+6=0$, so 2 has inverse 6 in $(\mathbb{Z}_8, +)$

The set $\{0,2,4,6\}$ is actually a subgroup of $\mathbb{Z}_8$

The set $\{0,4\}$ too is a subgroup.

There are no other subgroups of order 2 or 4

(nor 3,5,6,7 --- but that we know from Lagrange's thm..)

we found a (precisely one!) subgroup of order 2 and one of order 4 (*)

This (*) feature of $\mathbb{Z}_8$ is no coincidence: that's exactly what we should expect from cyclic groups of finite order:

Thm Let G be a cyclic group of order n, say $G = \langle g \rangle = \{e, g, \dots, g^{n-1}\}$. Then

(1) Every subgroup of G is cyclic

(2) If $1 \le k < n$ then g^k generates a subgroup of order $\frac{n}{\gcd(k,n)}$

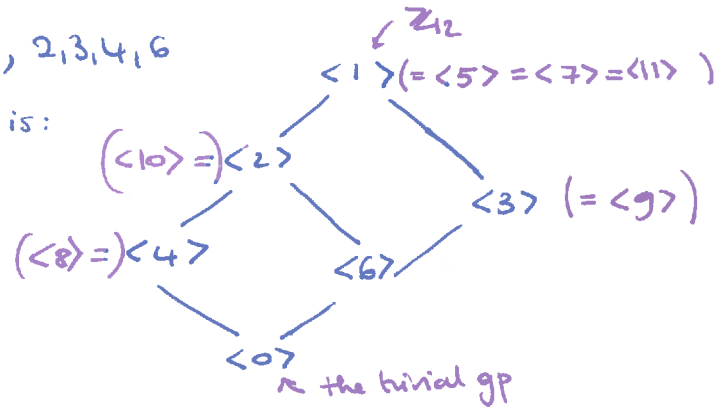
(3) For each positive divisor of n, G has exactly one subgroup of order d.

Rmk This theorem is telling us that the subgroup structure of finite cyclic groups is completely determined "arithmetically": it is enough to know the divisors of the order to know the subgroups of our group

Example $\mathbb{Z}_{12} = \{0,1,\dots,11\}$

divisors of 12 are: (1 & 12), 2, 3, 4, 6

The "subgroup lattice" of $\mathbb{Z}_{12}$ is:



Rmk We have seen in the example that each of the (sub)groups may have more than one generator. In particular, if $G = \langle g \rangle$ then $G = \langle g^k \rangle$ for any k coprime with n. These will play a role later, when considering – for instance – more than one operation on $\mathbb{Z}_n$.

The other result concerning the existence of subgroups of a prescribed order is the following.

Thm (Cauchy)

If G is a finite group and $p \in \mathbb{N}$ is a prime number (i.e. $p > 1$ & p is divisible by no positive integer other than 1 and itself.) which divides the order of G, then G contains an element of order p (and therefore a subgroup of order p).