2.3 Subgroups

[redacted]

Definition

A subset H of a group G is called a subgroup of G if H is itself a group using the group operation of G. We sometimes write $H < G$ to denote that H is a subgroup of G.

Theorem

Let G be a group and let $H \subseteq G$ with $H \neq \emptyset$. ($\subseteq$: subset (some authors write $\subset$ for subset))

$\subset$ and $\subseteq$ mean the same thing!

If:

(1) H is closed under compositions, i.e.,

$$a, b \in H \Rightarrow ab \in H$$

(ab: group operation in G)

(2) H is closed under inverses, i.e.,

$$a \in H \Rightarrow a^{-1} \in H$$

then H is a subgroup of G.

Proof:

We have to show that H is a group. We know that H is closed under compositions & inverses, so we just have to show that the operation in H is associative & that

H contains an identity.

But the operation is associative on G, so it must be associative on the smaller set H. That is, we know that

$$\forall a,b,c \in G \qquad (ab)c = a(bc).$$

But $H \subseteq G$, so we therefore have

$$\forall a,b,c \in H \qquad (ab)c = a(bc).$$

Next, since $H \neq \emptyset$, we know that there is some element $a \in H$. Since H is closed under inverses, we also have $a^{-1} \in H$. Therefore $e = aa^{-1} \in H$ (↑ ident. elem of G).

Further, e is the ident. element of H because

$$\forall a \in G, \quad ae = a = ea$$

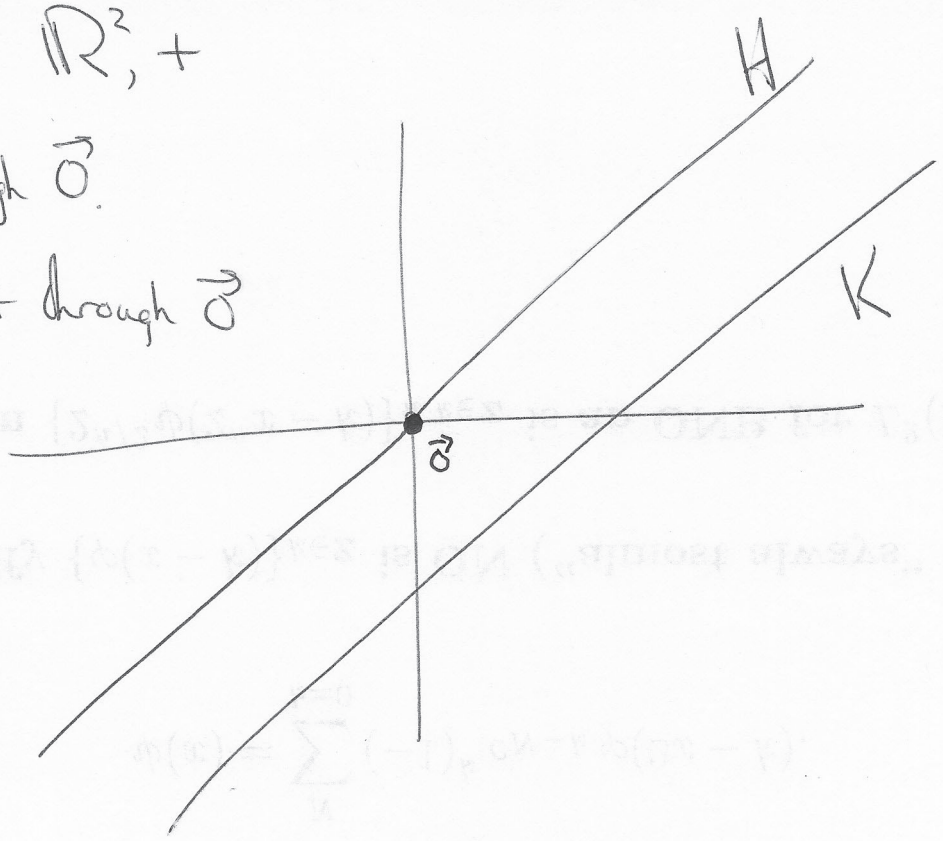
and therefore

$$\forall a \in H, \quad ae = a = ea. \qquad \blacksquare$$

Example $\mathbb{R}^2, +$

H = line through $\vec{0}$.

K = line not through $\vec{0}$



a. $\vec{0} \in H$ ✓ (hence nonempty)

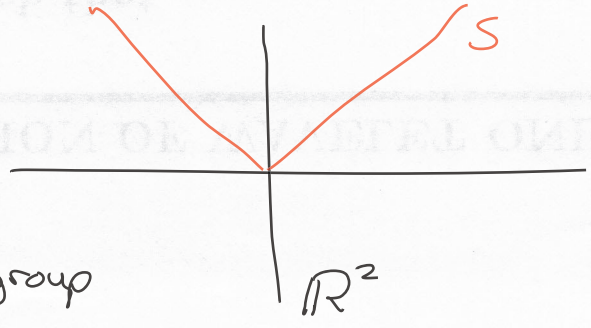
b. $\vec{x}, \vec{y} \in H \Rightarrow \vec{x}+\vec{y} \in H$ ✓

c. $\vec{x} \in H \Rightarrow -\vec{x} \in H$ ✓.

So, H is a <u>subgroup</u>.

But K is <u>not</u> a subgroup: does not contain the identity!

Exercise: Let S be:



Show that S contains the identity element, but S is <u>not</u> a subgroup

Exercise
If G is a group, then $\{e\}$ & G are subgroups of G, called the trivial subgroups.

Example
The set of all rationals $\mathbb{Q}$ is a group under $+$.
Let

$$H = \left\{ \frac{m}{2^n} : m, n \in \mathbb{Z} \right\}.$$ This is nonempty!

a. H is closed under addition since

$$\frac{m}{2^n} + \frac{j}{2^k} = \frac{2^k m + 2^n j}{2^{n+k}} \in H.$$

b. H is closed under inverses since

$$-\frac{m}{2^n} = \frac{-m}{2^n} \in H.$$

Thus H is a subgroup of G.

H is called the set of dyadic rationals.

Example $G = S_3 = \{$ all bijections of $\{1,2,3\}$ onto itself $\}$

Consider

Two-line notation: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Picture Notation:

Cycle Notation: $\sigma = (1\,2\,3)$

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad \sigma^2 = (1\,3\,2)$

$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad \sigma^3 = e$

$\sigma^4 = \sigma$, $\sigma^5 = \sigma^2$, $\sigma^6 = e$, etc.

$\sigma^{-1} = \sigma^2$, $\sigma^{-2} = \sigma^{-1}$, $\sigma^{-3} = e$, etc.

$H = \{\sigma, \sigma^2, e\}$ is nonempty, closed under compositions & inverses, so is a subgroup of S_3.

Note: $H = \{\sigma^n : n \in \mathbb{Z}\}$ ← looks like this could be an ∞ set, but it isn't! There are many duplicates!

But there are only 3 distinct functions in this set.

H is an example of a cyclic subgroup.

Definition
If G is a group, then the cyclic subgroup generated by a is

$$(a) = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

We'll show this is a subgroup, but note first that there are only two possibilities.

Case 1: $a^m = a^n$ for some integers $m < n$.

Then $e = a^m a^{-m} = a^n a^{-m} = a^{n-m}$

where $n - m > 0$. Thus $a^k = e$ for some finite $k > 0$.

There may be many such k, but there must be a smallest such $k > 0$. This k is called the

order of a, denoted

$$o(a) = k = \text{smallest } n > 0 \text{ s.t. } a^n = e.$$

In this case,

$$(a) = \langle a \rangle = \{e, a, \ldots, a^{k-1}\}$$ (Exercise: justify!)

Case 2. $a^m \neq a^n$ for any $m \neq n \in \mathbb{Z}$.

In this case

$$(a) = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

we say that a has infinite order, and write $o(a) = \infty$.

Exercise Show that if $a \in G$ then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Note that if G is a finite group then $\langle a \rangle$ must be a finite set, so a has finite order. If G is an infinite group then $\langle a \rangle$ could be finite or infinite.

Exercise
Suppose $a \in G$ has finite order, say $k = o(a)$. Show that

$$a^n = e \iff k \mid n.$$

Exercise: Show that $H = \left\{\frac{m}{2^n} : m, n \in \mathbb{Z}\right\}$ is not a cyclic subgroup of $\mathbb{Q}$.
(under the operation of addition)

Example: Center of G

Let G be a group. The center of G is the set Z(G) that contains all elements that commute with every other element:

$$Z(G) = \{ g \in G : gh = hg \ \forall h \in G \}.$$

Exercise: Show that Z(G) is a subgroup of G.

Exercise: If G is abelian, then Z(G) = G.

Consequently, if G is not abelian, then Z(G) is a proper subset of G. However, all this tells us is that the center is not ALL of G. The center could be a very "small" subgroup of G, or it could be a large but still proper subgroup. If Z(G) is "large", then in some sense the group G is "nearly abelian", while if Z(G) is "small" then G is "very nonabelian". These are imprecise terms, but the point is that by looking at the center we can get some idea of just "how nonabelian" a nonabelian group is.

Example: Centralizer of a

If G is any group & $a \in G$, then the centralizer of a is

$$C(a) = \{g \in G : ga = ag\}$$

That is, $C(a)$ contains those elements $g \in G$ that commute with a.

If $g, h \in C(a)$, then

$$\begin{aligned}(gh)(a) &= g(ha) = g(ah) \\ &= (ga)h \\ &= (ag)h \\ &= a(gh).\end{aligned}$$

Thus $gh \in C(a)$, so $C(a)$ is closed under compositions.

Exercise: Show $C(a)$ is a subgroup of G.