Chap 3: Definition of groups

Def. a group is a set G with an operation $*$ that satisfies 3 axioms: $(G1)$: $*$ is associative

$(G2)$: there is an identity element e : $a*e=e*a=a \ \forall a \in G$

$(G3)$: $\forall a \in G$, $\exists$ an element $a^{-1} \in G$ s.t. $a*a^{-1}=a^{-1}*a=e$.

Examples: 1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$;

$(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_{>0},\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_{>0},\times)$.

There are commutative groups: $a*b=b*a \ \forall (a,b) \in G \times G$.

$(\mathbb{Z}_{>0},\times)$, $(\mathbb{Q},\times)$ are not groups.

2. $(\mathbb{Z}_n,+) = (\{0,1,2,\cdots,n-1\}$, addition modulo $n)$

$(\mathbb{Z}_3,+)$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

commutative groups are also called abelian groups.

$(\mathbb{Z}_3^*,\times)$:

×	1	2
1	1	2
2	2	1

$(\mathbb{Z}_5^*,\times)$:

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_n^*,\times)$ is a group $\Leftrightarrow$ n is a prime number

$\|$

$(\{1,2,\cdots,n-1\}$, multiplication modulo $n\}$

3. $x*y=x+y+a$ on $\mathbb{R}$ is an abelian group.

$e=-a$. $x^{-1}=-2a-x$.

$x*y=\frac{xy}{2}$ on $\mathbb{R}$ is an abelian group $e=2$

$x^{-1}=\frac{4}{x}$

4. $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $B=\begin{pmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ +\sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}$

claim: $\begin{matrix}\boxed{AB^2=BA}\\ \parallel\\ \begin{pmatrix}-\frac{\sqrt{3}}{2} & -\frac{1}{2}\\ -\frac{1}{2} & \frac{\sqrt{3}}{2}\end{pmatrix}\end{matrix}$

$B^2=\begin{pmatrix}\cos\frac{4\pi}{3} & -\sin\frac{4\pi}{3}\\ \sin\frac{4\pi}{3} & \cos\frac{4\pi}{3}\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & \frac{\sqrt{3}}{2}\\ -\frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}$

$\boxed{A^2=I,\ \ B^3=I}$

$G=\{I, A, B, B^2, AB, BA\}$

operation table:

	I	A	B	B^2	AB	BA
I	I	A	B	B^2	AB	BA
A	A	I	AB	BA	B	B^2
B	B	BA	B^2	I	A	AB
B^2	B^2	AB	I	B	BA	A
AB	AB	B^2	BA	A	I	B
BA	BA	B	A	AB	B^2	I

e.g: $B\,BA=B\cdot AB^2$

$=AB^2B^2=AB$

$B^2AB=(B^2A)\cdot B$

$=AB\cdot B=AB^2$

$=BA$

$ABA=AAB^2=B^2$

$ABAB=B^3=I$

$(AB)(BA)=AB^2A=BAA=B$

$BAB=AB^2B=A$

$G=\langle A, B \mid A^2=B^3=I,\ AB^2=BA\rangle$

5. $(a,b)*(c,d)=(ac, bc+d)$ on $\mathbb{R}^2 \setminus \{x=0\}$

Check:

(G1) $((a,b)*(c,d))*(e,f)=(ac, bc+d)*(e,f)=(ace, (bc+d)e+f)$ ✓

$$\|$$

$(a,b)*((c,d)*(e,f))=(a,b)*(ce, de+f)=(ace, bce+de+f)$

(G2) $(a,b)*\underset{\overset{\|}{e}}{\underline{(c,d)}}=(ac, bc+d)=(a,b)$ for any $(a,b)\in\mathbb{R}^2$

$\Leftrightarrow c=1, d=0.$

$(c,d)*(a,b)=(ca, da+b)=(a,b)$ for any $(a,b)\in\mathbb{R}^2$

$\Leftrightarrow c=1, d=0$

so there exists an identity $e=(1,0)$.

(G3) $(a,b)*(c,d)=(ac, bc+d)=(1,0) \Leftrightarrow c=a^{-1}, d=-ba^{-1}$.

$(a^{-1}, -ba^{-1})*(a,b)=(1, -ba^{-1}a+b)=(1,0)=e$

$\Rightarrow (a,b)^{-1}=(a^{-1}, -ba^{-1})$.

So $(\mathbb{R}^2\setminus\{x=0\}, *)$ is a group.

$(a,b)*(c,d)=(ac, bc+d)$ $\Rightarrow$ non-abelian gp.

✗

$(c,d)*(a,b)=(ca, da+b)$

$(\mathbb{R}^2, *)$ is not a group because $(0,b)$ has no inverse.

6. groups of subsets of a set.

Let D be a set. The power set of D is the set of all the subsets of D. denoted by $P_D = \{A : A \subseteq D\}$.

Ex: $D=\{a,b\} \Rightarrow P_D = \{\phi, \{a\}, \{b\}, \{a,b\}\}$.

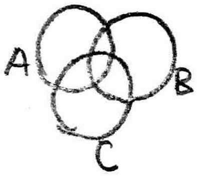
D is a finite set with n elements $\Rightarrow \# P(D) = 2^n$.

$\#D = n$

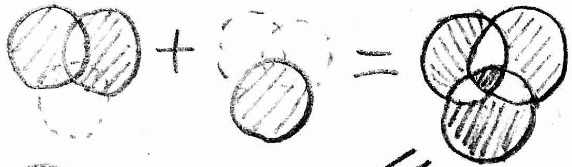
For any $A, B \in P_D$,
Define $A+B = (A-B) \cup (B-A)$ (symmetric difference)

Then $(P_D, +)$ is a group. which is commutative.

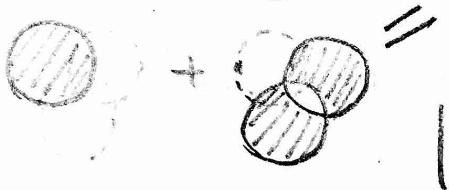
(G1):



$(A+B)+C =$



$A+(B+C) =$



(G2). (G3) exercise

$\left|\frac{x+y}{1+xy}\right| < 1$

$\Uparrow$

7. $x*y = \frac{x+y}{xy+1}$ on $(-1,1)$ $\quad x, y \in (-1,1) \Rightarrow x*y \in (-1,1)$

(G1): $(x*y)*z = \frac{x+y}{xy+1} * z = \frac{\frac{x+y}{xy+1}+z}{\frac{x+y}{xy+1}z+1} = \frac{x+y+(xy+1)z}{(x+y)z+xy+1} = \frac{x+y+z+xyz}{xy+yz+xz+1}$

$x*(y*z) = x*\frac{y+z}{yz+1} = \frac{x+\frac{y+z}{yz+1}}{x\frac{y+z}{yz+1}+1} = \frac{x(yz+1)+y+z}{x(y+z)+yz+1}$ //

(G2) $\frac{x+y}{xy+1} = x \ \forall x \iff y=0. \Rightarrow 0$ is the identity elem

(G3) $\frac{x+y}{xy+1} = 0 \iff y=-x. \Rightarrow x^{-1} = -x$

$\left((1+xy)^2-(x+y)^2 = 1+2xy+x^2y^2-x^2-y^2-2xy = (1-x^2)(1-y^2) > 0 \Rightarrow \left|\frac{x+y}{1+xy}\right| < 1 \right)$