Introduction to abstract algebra

Def: A group is a triple $(G, \cdot, e)$ where G is a set and "$\cdot$" is a binary operation on G, such that the following hold

(a) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$

(b) $e \cdot x = x \cdot e = x$ for all $x \in G$

(c) For every $x \in G$ there exists $y \in G$ such that $x \cdot y = y \cdot x = e$

e is called the identity, and it is common to omit the symbol "$\cdot$"; G is called an Abelian group if the following holds

(d) For all $x, y \in G$ we have $x \cdot y = y \cdot x$.

very often, the operation symbol in an Abelian group is chosen to be '+', and in this case the identity is called 0. Usually, we find e to be exchanged by 1.

If in the above setting only (a) holds, we call G a <u>semigroup</u>; if (a) and (b) hold, we speak about a <u>monoid</u>.

<u>Examples</u> a) $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), \dots$

b) $(\mathbb{Q}-\{0\}, \cdot, 1), \dots$

c) $\mathbb{Z}_n^\times := \{k \in \{0, \dots, n-1\} \mid \gcd(k,n) = 1\}$ together with multiplication modulo n

d) $\mathbb{Z}_n = \{0, \dots, n-1\}$ together with addition modulo n.

e) $M_2^\times(\mathbb{Q}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Q},\ ad - bc \neq 0 \right\}$ together with matrix multiplication.

This is a non-Abelian example.

Def. Let G be a group and let $x \in G$.

We define $x^n := \underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ factors}}$

and it is easily verified, that $x^n \cdot x^m = x^{n+m}$ and $(x^n)^m = x^{n \cdot m}$

Finally $x^n \cdot x^m = x^m \cdot x^n$ which can be quite useful.

Proposition a) The identity is unique, ie if there is $f \in G$ with $f \cdot x = x = x \cdot f$, then $f = e$.

b) The inverse is unique, i.e. if $a \cdot b = b \cdot a = e$ and $a \cdot c = c \cdot a = e$, then $b = c$.

c) Calling this unique inverse a^{-1}, we have $(a^{-1})^{-1} = a$.

Proof a) We have $e = e \cdot f = f$, the first equality because f is an identity, the second, because e is an identity.

b) We have $b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c$
$= e \cdot c = c$.

c) This is evident, as $a \cdot a^{-1} = e = a^{-1} \cdot a$ so a must be the inverse of a^{-1}, and this means $a = (a^{-1})^{-1}$.

The operation table of a group is also known under the name Cayley table. Here are a few examples: $(\mathbb{Z}_2, +, 0)$

+	0	1
0	0	1
1	1	0

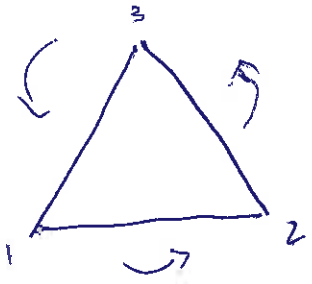
Another one is this $(\mathbb{Z}_5, +, 0)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

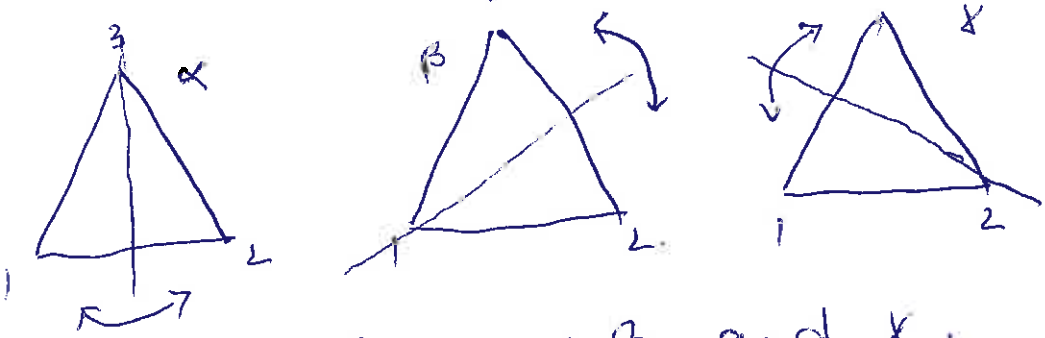
The fact that these examples are Abelian directly shows that the tables must be symmetric around the main diagonal. Here a final example $(\mathbb{Z}_5^{\times}, \cdot, 1)$ see also first examples after Def of a group.

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

All these examples so far are Abelian and we wonder about a smallest non-Abelian example; this can be easily obtained by looking at the symmetries of an equilateral triangle.



We have the identity e that does not move anything; then there are two rotations, one by 120° and the other by 240°. Let's call them ρ and ρ^2. Finally we need to discuss reflections



We will call them α, β, and γ. Observe, that $\rho^3 = e = \alpha^2 = \beta^2 = \gamma^2$. Now let us compose the Cayley table

$\cdot$	e	ρ	ρ^2	α	β	γ
e	e	ρ	ρ^2	α	β	γ
ρ	ρ	ρ^2	e			
ρ^2	ρ^2	e	ρ			
α	α			e		
β	β				e	
γ	γ					e

These entries are obvious or follow from the above so far.

	e	ρ	ρ^2	α	β	γ
e	e	ρ	ρ^2	α	β	γ
ρ	ρ	ρ^2	e	γ	α	β
ρ^2	ρ^2	e	ρ	β	γ	α
α	α	β	γ	e	ρ	ρ^2
β	β	γ	α	ρ^2	e	ρ
γ	γ	α	β	ρ	ρ^2	e

Inspection of the combined reflections and rotations we first find that $\rho \cdot \alpha = \gamma$.

After this, the second row has only two positions empty for the results of $\rho \cdot \beta$ and $\rho \cdot \gamma$. The values for these must come from $\{\alpha, \beta\}$ because all other elmts already occur in the second row. If we set $\rho \cdot \beta = \beta$ then we would get $\rho = e$, which we know is not the case, hence

$\rho \cdot \beta = \alpha$ and $\rho \cdot \gamma = \beta$.

Inspection shows further that $\alpha \cdot \rho = \beta \neq \gamma$ so we see the group is not Abelian. The already entered elmts then help to fill the second column. The 3rd row and column are filled easily with these results so far, so only the 3×3 block in the lower right corner is left; computing $\alpha \cdot \beta = \rho$ fills it up.

Def Let G be a group and $\emptyset \neq H \subseteq G$ a subset of G. We say H is a subgroup of G, formally $H \leq G$, if H is closed under the operation on G and satisfies all group axioms.

Examples a) G itself and also $\{e\}$ are called the trivial subgroups of G

b) $2\cdot\mathbb{Z} = \{2\cdot z \mid z \in \mathbb{Z}\}$ = "even numbers" form a subgroup of $(\mathbb{Z}, +, 0)$

c) $H := \{e, s, s^2\}$ is the subgroup of all rotations in the group discussed earlier (non-Abelian 6-element group)

We are of course interested in simple criteria that may be checked in order to verify the subgroup property. For this a few preparational statements are useful.

Lemma: Let G be a group with identity e. If $x \in G$ satisfies $x^2 = x$ then $x = e$

proof. $x = ex = (x^{-1}x)x = x^{-1}(xx) = x^{-1}x = e$

Corollary: Let H be a subgroup of the group G with identity e. Then $e \in H$.

proof: H as a subgroup must have an identity, say $f \in H$. But then $f^2 = f$ and this not only in H but of course also in G. Then according to the lemma we find $f = e$.

Proposition: A subset H of a group G is a subgroup, if and only if the following hold

(a) $H \neq \emptyset$

(b) $a, b \in H$ implies $a \cdot b \in H$

(c) If $a \in H$ then $a^{-1} \in H$

This can even be shortened to the two criteria

(a) $H \neq \emptyset$

(b) $a, b \in H$ implies $ab^{-1} \in H$.