Abstract Algebra – II Groups (群理论)

Melchior Grützmann / 古梅西
melchiorG.freehosting.com/algebra

October 15, 2012

Outline

Normal subgroups (正规子群) III

Example

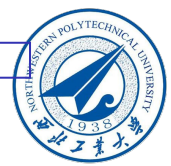
Given again the subgroup $A_3 \triangleleft S_3$, we have already proved that it is a normal subgroup. The two cosets are A_3 and $S_3 \setminus A_3 = (12)A_3$. Therefore the group structure on S_3/A_3 is just $(\{\pm 1\}, \cdot)$.

Corollary

Given a normal subgroup $N \triangleleft G$, then the subgroups of G/N are in 1:1-correspondence with subgroups $\{S \subset G : N \subset S\}$.

Proof.

Let us denote $\pi\colon G \to G/N$ the projection. Given a subgroup $S \subset G$, then it projects onto a subgroup $\pi(S) \subset G/N$. Conversely, given $S' \subset G/N$ then it comes from a subgroup $\pi^{-1}(S') \subset G$ that contains $N = \pi^{-1}(\mathrm{id}')$. To see that this is the only subgroup containing N and projecting onto S', note that $\pi(g) \in S'$ is equivalent to $gN \in S$. But then all of gN must be contained in the subgroup $S \subset G$ that projects onto S'. □



Normal subgroups (正规子群) IV

Corollary

Given a normal subgroup $N \triangleleft G$, then π and π^{-1} map inclusions to inclusions (i.e. $N \subset S_1 \subset S_2 \subset G$, then $\pi(S_1) \subset \pi(S_2)$ and the analogue for π^{-1}) and normal subgroups onto normal subgroups (i.e. $K \triangleleft G$ implies $\pi(K) \triangleleft G/N$).

The proof of preservation of normality is left as an exercise.

Center, Centralizer, and Normalizer

In the search for normal subgroups we also obtain the following two notions:

Definition

Given a group G, then we define

1. *The center (中心) of G as*
   $\operatorname{cent} G := \{z \in G : \forall g \in G : zg = gz\}$,
2. *Given an abelian subgroup $H \subset G$ the centralizer (中心化子)*
   $\operatorname{cent}_G H := \{g \in G : \forall h \in H : gh = hg\}$,
3. *Given a subgroup $H \subset G$ its normalizer (正规化子)*
   $N_G(H) := \{g \in G : gH = Hg\}$.

Center, Centralizer, and Normalizer II

Example

Consider the group D_4. Its center is trivial, i.e. $\{\mathrm{id}\}$ as the multiplication table shows. Consider further its subgroup $H = \langle \sigma_A \rangle = \{\mathrm{id}, \sigma_A\}$. It is not normal, because $\sigma_a H \neq H\sigma_a$, but it is abelian. Its centralizer is $\mathrm{cent}_{D_4} H = \langle \sigma_A, \sigma_B, \tau^2 \rangle$ and its normalizer is also $N_{S_4}(H) = \langle \sigma_A, \sigma_B, \tau^2 \rangle$.

Remark

Given a group G, then its center is a normal abelian subgroup. Given an abelian subgroup $H \subset G$, then its centralizer is the biggest subgroup of elements commuting with all elements of H. (In particular $H, \mathrm{cent}(G) \subset \mathrm{cent}_G(H)$.) Given any subgroup $H \subset G$, then its normalizer is the biggest subgroup in which H is a normal subgroup.

Endomorphisms (自同态) and Automorphisms (自同构)

Definition

Given a group G, then the endomorphisms *(自同态)* $\mathrm{End}(G)$ *are the homomorphism of G into itself.*
The automorphisms *(自同构)* $\mathrm{Aut}(G)$ *are the isomorphisms of G onto itself.*

Note that the endomorphisms form a monoid while the automorphisms form a group.

Example

Consider $C_3 = \mathbb{Z}/(3) = \langle [1] \rangle$. Obviously any endomorphism is specified by the image of $[1]$. The endomorphisms are therefore $\{[0], [1], [2]\}$ with the operation $\cdot$ (multiplication), the identity $\mathrm{Id}_{C_3} = [1]$. The automorphisms are those endomorphisms that are invertible, i.e. $\mathrm{Aut}(C_3) = \{[1], [2]\} = \mathrm{End}(C_3)^*$ under the same operation.

Summary: The study of groups means the study of group structure together with the subgroup structure, endo-, iso-, and other homomorphisms (to and from groups).

Exercises V

Exercise

Prove that the union of an increasing sequence of normal subgroups $N_1 \subset N_2 \subset N_3 \subset \cdots \subset G$, $N_i \triangleleft G$ of a group G is normal $\bigcup_i N_i \triangleleft G$.

Exercise

a. Let G be a group generated by $X \subset G$. Prove that for two homomorphisms $\phi, \psi \colon G \to H$ into any group H, $\phi(x) = \psi(x)$ for all $x \in X$ is equivalent to $\phi = \psi$.

b. Find all endomorphisms of $V_4 := \langle (12)(34), (13)(24), (14)(23) \rangle \subset S_4$ (Klein's four group).

c. Find all automorphisms of V_4.

d. Find all endomorphisms and automorphisms for D_3.

2.3 Isomorphism theorems (双同态定理)

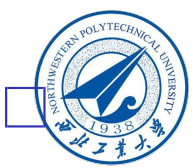
The quotient map $G \mapsto G/N$ of a group G by a normal subgroup $N \triangleleft G$ gives an example of a universal map (也泛性质) in the following way.

Proposition

Let $N \triangleleft G$ be a normal subgroup. Then every homomorphism $\phi\colon G \to H$ whose kernel contains $N \subset \ker\phi$ factors uniquely through the quotient map $\pi\colon G \to G/N$, i.e. there is a unique group homomorphism $\bar{\phi}\colon G/N \to H$ such that $\phi = \bar{\phi} \circ \pi$.

Proof.

Idea $\bar{\phi}(gN) := \phi(g)$, but first check representation independence. Let thus $gN = hN$ for some $g, h \in G$. But then $\phi(g) = \phi(gN) = \phi(hN) = \phi(h)$ and thus $\bar{\phi}$ is well defined. The homomorphism properties follow now from those of ϕ. The last property follows from the definition of $\bar{\phi}$.



Theorem (First isomorphism theorem)

Given a group homomorphism $\phi\colon G \to H$, then $G/\ker\phi \cong \operatorname{im}\phi$.

Proof.

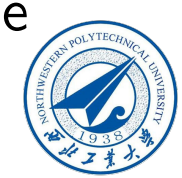
The obvious candidate for the isomorphism is $\bar{\phi}\colon G/\ker\phi \to \operatorname{im}\phi : g\ker\phi \mapsto \phi(g)$. First let us check that $\bar{\phi}$ is well defined. Let thus $N := \ker\phi$ and $gN = hN$ for some $g, h \in G$. But then $\phi(g) = \phi(gN) = \phi(hN) = \phi(h)$ and thus the image is the same. Second, note that $gN \in \ker\bar{\phi}$ implies $\bar{\phi}(gN) = \phi(g) = \mathrm{id}' \in H$ and thus $g \in N$. Therefore $\bar{\phi}$ is injective. Finally note that every $h \in \operatorname{im}\phi$ has a $g \in G$ with $\phi(g) = h$. But then $\bar{\phi}(gN) = h$ and thus $\bar{\phi}$ is also surjective and therefore bijective, i.e. an isomorphism. □

Application: cyclic groups I

Example

Let $g \in G$ be an element, then $\langle g \rangle$ is cyclic. Consider the map $\phi\colon \mathbb{Z} \to G : n \mapsto g^n$.
If $m > n \in \mathbb{N}$ with $g^m = g^n$, then $g^{m-n} = \mathrm{id}$. Let now N be the smallest such difference. Then $g^m = \mathrm{id}$ for every $N|m$ and thus $\bar{\phi}\colon \mathbb{Z}/(N) \to \langle g \rangle$ is well-defined, maps $1 \mapsto g$ and thus also surjective. Moreover $\ker \phi = \mathbb{Z}/(N)$ and thus $\bar{\phi}$ is also injective, thus an isomorphism.
If there is no $m > n \in \mathbb{N}$ with $g^m = g^n$, then all the g^m are disjoint, moreover they are also disjoint from g^{-m} for any $m \in \mathbb{N}$. Thus $\phi\colon \mathbb{Z} \to \langle g \rangle$ is a homomorphism, surjective, and also injective. Therefore $\mathbb{Z} \cong \langle g \rangle$.

In particular every two cyclic groups of order n are isomorphic. We denote by C_n the cyclic group of order n.



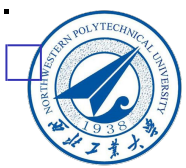
Subgroups of cyclic groups

Proposition

For a cyclic group of order n there is for every divisor $d|n$ a unique subgroup of order d.

Proof.

Let $C_n = \langle g \rangle$ be a cyclic group and g of order n. Define $S_d := \langle g^{n/d} \rangle$. Clearly S_d is a cyclic group which moreover has d elements, because for $h_0 := g^{n/d}$, $h_0^{d'} = \mathrm{id}$ with $0 \leq d' < d$ would imply that h has order less than d and thus g order less than n which contradicts the assumption. Conversely it is also possible to define a set $S'_d := \{h \in G : h^d = \mathrm{id}\}$, i.e. all those elements for which d is an exponent. But since $\langle g \rangle = G$ for every $h \in S'_d$ there is an $m \in \mathbb{N}$ such that $h = g^m$. $h^d = \mathrm{id}$ implies $dm \equiv 0 \pmod{n}$, i.e. $dm = kn$ for some $k \in \mathbb{N}$. But then $m = k\frac{n}{d}$ and thus $h = h_0^k$, i.e. $h \in S_d$ and thus $S'_d \subset S_d$. The other inclusion is obvious, and thus $S_d = S'_d$, i.e. both definitions coincide and the subgroup S_d is unique (i.e. independent of $g \in G$ as long as $\langle g \rangle = G$). □

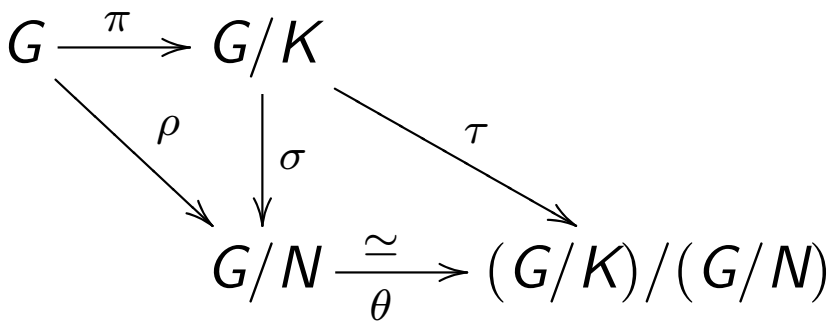


Theorem (Second isomorphism theorem)

Let G be a group and $N, K \triangleleft G$ be normal subgroups. If $K \subset N$, then $K \triangleleft N$, $N/K \triangleleft G/K$ and

$$(G/K)/(N/K) \cong G/N.$$

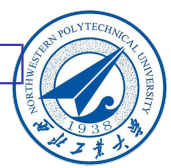
Idea: $K \subset N \triangleleft G$ induce the following maps



Proof.

Let $\pi\colon G \to G/K$ and $\rho\colon G \to G/N$ be the quotient maps. We show that there is a unique isomorphism $\theta\colon G/N \to (G/K)/(N/K)$ such that $\theta \circ \rho = \tau \circ \pi$ where we also need to show that there is a morphism $\tau\colon G/K \to (G/K)/(N/K)$.

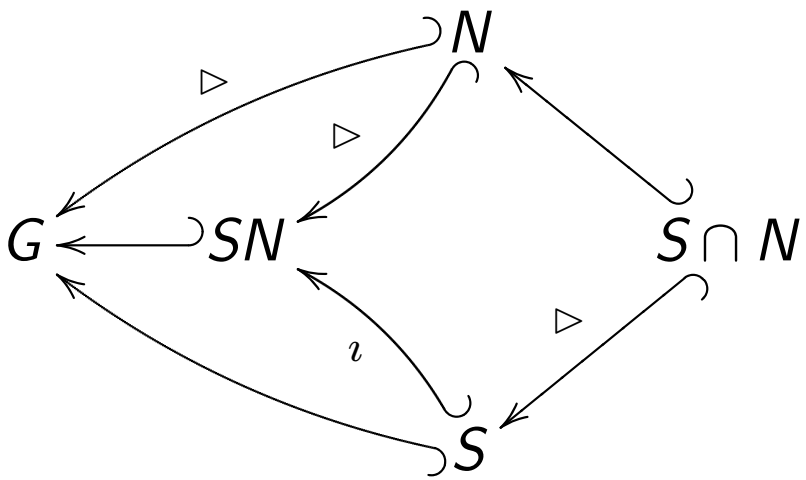
First note that ρ factors through π, because $K \subset N$, i.e. there is some homomorphism $\sigma\colon G/K \to G/N : gK \mapsto gN$ such that $\rho = \sigma \circ \pi$. Since ρ is surjective, so is σ. We show that $\ker\sigma = N/K$. First note that $K \lhd N$, because $K \lhd G$. For $n \in N$ we have $\sigma(nK) = nN = N$. Conversely if $\sigma(gK) = N$, then $gN = N$ and thus $g \in N$. This shows $\ker\sigma = N/K$. Therefore in particular $N/K \lhd G/K$. Now the first isomorphism theorem yields an isomorphism $\theta\colon G/N \xrightarrow{\simeq} (G/K)/(N/K)$ such that $\theta \circ \sigma = \tau$. Then $\theta \circ \rho = \tau \circ \pi$. Since ρ is surjective, θ is unique with this property. This completes the proof. □



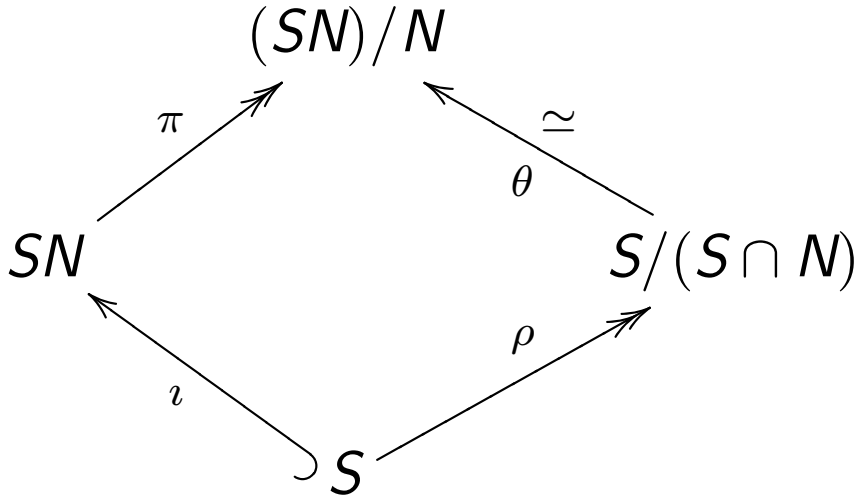
Proposition (Third isomorphism theorem)

Given a group G together with a subgroup $S \subset G$ and a normal subgroup $N \triangleleft G$, then $SN \subset G$ is a subgroup, $S \cap N \triangleleft S$ is a normal subgroup of S, and $S/(S \cap N) \cong (SN)/N$.

Subgroup inclusion pattern:



The required maps are:



I.e. the arrows to the down-left indicate normal subgroups, the others are just subgroups, and the groups to the right (along an arrow) are subgroups of the groups to the left.

Proof.

First note that $SN \subset G$ is indeed a group, because N is normal. Moreover $N \triangleleft (SN)$. We will show that there is a unique isomorphism $\theta\colon S/(S \cap N) \to (SN)/N$ such that $\theta \circ \rho = \pi \circ \imath$ where $\pi\colon SN \to (SN)/N$ is the projection, $\imath\colon S \hookrightarrow SN$ the inclusion, and there is a surjective homomorphism $\rho\colon S \to S/(S \cap N)$.
Let $\phi\colon S \to (SN)/N : s \mapsto sN$, i.e. $\phi = \pi \circ \imath$ and ϕ is surjective. Moreover $\phi(g) = N$ iff $g \in N$, i.e. $\ker \phi = S \cap N$ which is therefore normal in S. Therefore ρ is just the canonical projection (and in particular surjective). Again by the first isomorphism theorem $(SN)/N = \operatorname{im} \phi \cong S/\ker \phi = S/(S \cap N)$, i.e. there is an isomophism $\theta\colon S/(S \cap N) \xrightarrow{\simeq} (SN)/N$. Moreover the isomorphism constructed in the proof of the theorem fulfills $\theta \circ \rho = \phi = \pi \circ \imath$ and is thus unique, because ρ is surjective. This completes the proof. □

Application: This implies in particular that the intersection of two normal subgroups of finite index has finite index.

Exercises I

Exercise

Let $\phi\colon A \to B$ and $\psi\colon A \to C$ be group homomorphisms. Prove the following: If ψ is surjective, then ϕ factors through ψ if and only if $\ker\psi \subset \ker\phi$. In this case ϕ factors uniquely through ψ.

Exercise

Show that the identity homomorphism $\mathrm{Id}\colon 2\mathbb{Z} \xrightarrow{\sim} 2\mathbb{Z}$ does not factor through the inclusion homomorphism $\imath\colon 2\mathbb{Z} \hookrightarrow \mathbb{Z}$ even though $\ker\imath \subset \ker\mathrm{Id}$.
Hint: Opposite to the situation in Exercise 3.1, $\imath$ is not surjective.

Exercise

Let $\phi\colon A \to C$ and $\psi\colon B \to C$ be group homomorphisms. Prove the following: If ψ is injective, then ϕ factors through ψ if and only if $\mathrm{im}\,\phi \subset \mathrm{im}\,\psi$. In this case ϕ factors uniquely through ψ.

Exercises II

Exercise

Show that every subgroup of a cyclic group is cyclic.

Exercise

a. Show that the additive group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the multiplicative group of all complex numbers $\mathbb{C}$ of modulus 1.

b. Show that the additive group $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the group of all complex roots of unity (i.e. all complex numbers $z \neq 0$ such that $\langle z \rangle$ is finite in $\mathbb{C}^*$).

c. Show that the complex n-th roots of unity $\Omega_n := \{z \in \mathbb{C} : z^n = 1\}$ form a cyclic group (w.r.t. multiplication).

Exercises III

Exercise

Consider the group $D_4 := \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^4, \sigma\tau\sigma = \tau^{-1} \rangle$

a. Find the order of every element in D_4,

b. Show that for every $d | (D_4 : 1)$ there is a subgroup $S \subset D_4$ of order d.

Exercise

a. Let G be a finite group and $S, T \subset G$ any subgroups. Show that $|ST| = |S|\,|T|/|S \cap T|$.

b. Find a group G together with subgroups $S, T \subset G$ such that $ST \subset G$ is not a group.

Exercises IV

Exercise

Let G be a finite group, $N \triangleleft G$ a normal subgroup and $H \subset G$ any subgroup such that $|N|$ and $(G : N)$ are relatively prime. Show that $H \subset N$ iff $|H|$ divides $|N|$.
Hint: Consider $HN \subset G$.

Free groups (自由群), free products (自由的群积), and presentations (群的展示)

Example

Consider the group $\mathbb{Z}/(4)$ it can be generated by the element $[1]$ (as well as $[3]$), because $[1]+[1]=[2], [1]+[2]=[3], [1]+[3]=[0]$. Moreover the elements fulfill the trivial relations $a+(b+c)=(a+b)+c$, $[0]+a=a=a+[0]$, as well as $b+a=a+b$, $4a:=a+a+a+a=0$ and infinitely many more.

Definition

A presentation of a group is a set S of generators together with a set R of relations between them. Notation $G=\langle s\in S : R\rangle$ where we understand associativity and the role of the neutral element and inverse elements to be implied.

Free groups (自由群)

Lemma (引理)

Given a finite set S of generators there is a group $F(S)$ that is generated by S and for every map $\phi\colon S \to G$ into a group G there is a unique group homomorphism $\tilde{\phi}\colon F(S) \to G$.

Example

1. These groups are called *free groups* and the simplest example of a free group is $F_1 = \mathbb{Z}$ generated by 1. This is a cyclic group.
2. The free group on the generators S is (isomorphic to) the set of all (finite) cancelled words in $S \cup \bar{S}$. A word $abc\ldots z$ is called cancelled if there are no adjacent $a\bar{a}$ or $\bar{a}a$ for any $a \in S$. The group operation is concatenation together with canceling, i.e. $a\bar{a} \mapsto \epsilon$, $\bar{a}a \mapsto \epsilon$ for all $a \in S$.

Theorem

Given a set S of generators and a set of relations (代数关系) R in elements of S, then there is a group generated by S that fulfills only the relations $\langle R \rangle_S$.

Sketch of the proof.

The idea is to start from the free group $F(S)$ and to impose the relations R. In order to do that we consider the normal subgroup $\langle R \rangle_S \triangleleft F(S)$ that is generated by R. The quotient is clearly a group generated by the images of S. □

Example

1. The dihedral group is $D_n := \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^n, \sigma\tau\sigma = \tau^{-1} \rangle$.
2. The cyclic groups $\mathbb{Z}/(n) \cong \langle 1 : n \cdot 1 = 0 \rangle$.

Quaternions

The *quaternions* (四元数) are defined as $\mathbb{H} := \mathbb{R}(i, j, k)$ where the unit quaternions i, j, and k multiply as $i^2 = -1 = j^2 = k^2$ and $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$. These units form a group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Obviously Q is generated by i and j, also $i^4 = 1$ and $i^2 = j^2$. But we also have the relation $jij^{-1} = i^{-1}$. We want to show that these three generate all relations in Q, i.e. that $Q \cong \langle i, j : i^4 = \mathrm{id}, i^2 = j^2, jij^{-1} = i^{-1} \rangle$. Denote the second group by Q' and note that every element in Q' can be written as a finite sequence of is and js. Combining adjacent is to i^m and js to j^n, we see that $0 \leq m, n \leq 3$. Moreover the last relation ($ji = i^{-1}j$) permits us to move every i to the left of all j. Therefore we are left with at most 16 elements. But we also see that we can replace j^2 by i^2 and thus j^3 by $i^2 j$. Therefore we are left with 8 elements which are exactly the elements of Q and thus $Q' = Q$.

Corollary

If G is a group generated by a subset $S \subset G$, then there is a unique surjective homomorphism $\phi\colon F(S) \to G$ that is the identity on S. □

Corollary (Free product – 自由的群积)

Given two groups G and H – where we assume $G \cap H = \{\mathrm{id}\}$ – there is a unique group $G * H$ that has $G \cup H$ as generators and fulfills only the relations $\langle R_G, R_H \rangle_{G \cup H}$. □

Example

Given two free groups F_m and F_n then their free product $F_m * F_n \cong F_{m+n}$ is another free group.

Remark

A bit more difficult to show is that a subgroup of a free group is again a free group (possibly in 0 generators).

amalgamation (共合积)

$G \cap H = S$ a joint subgroup. Denote $\gamma\colon G \hookrightarrow G * H$ and $\theta\colon H \hookrightarrow G * H$ the inclusions into the free product. Then $G *_S H = G * H / \langle \gamma(s)\theta(s^{-1}) : s \in S \rangle_{G*H}$, i.e. the amalgamation of G and H over S is the quotient of the free product by the normal subgroup spanned by the anti-diagonal embedding of the intersection. It can be shown for $\bar{\gamma}\colon G \to G *_S H$ and $\bar{\theta}\colon H \to G *_S H$ that $G *_S H$ is generated by $\bar{\gamma}(G) \cup \bar{\theta}(H)$ and $\operatorname{im}\bar{\gamma} \cap \operatorname{im}\bar{\theta} = \bar{\gamma}(S) = \bar{\theta}(S)$.

Analogously to the free product, the amalgamated product fulfills the *universality property*: For every pair of group homomorphisms $\phi_G\colon G \to U$ and $\phi_H\colon H \to U$ such that $S = G \cap H$ and $\phi_G(S) = \phi_H(S)$, there is a unique $\tilde{\phi}\colon G *_S H \to U$ such that $\phi_G = \tilde{\phi} \circ \gamma$ and $\phi_H = \tilde{\phi} \circ \theta$.

Exercise

Given a group G, the conjugates of an element $x \in G$ are $C_x := \{gxg^{-1} : g \in G\}$. Given a subset $S \subset G$, there exists a smallest normal subgroup $N \triangleleft G$ that contains $S \subset N$. Show that N consists of all products of elements in $C_{S \cup S^{-1}}$.

Exercise

a. List (compactly) all elements of the group $\langle a, b : a^2 = \mathrm{id} = b^2 \rangle$. Give a compact multiplication table of the group.

b. List all elements of the group $\langle a, b : a^2 = \mathrm{id} = b^2 = (ab)^3 \rangle$ and give their multiplication table. Which known group is it isomorphic to?

Exercise

The multiplication of the unit quaternions $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ together with $\mathbb{R}$-linearity implies for $a, b, c, d, a', b', c', d' \in \mathbb{R}$,

$$\begin{aligned}(a + bi + cj + dk)(a' + b'i + c'j + d'k) = \\ =(aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i \\ + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k.\end{aligned}$$

a. Show that the multiplication is associative.

b. Let $\overline{a + bi + cj + dk} := a - bi - cj - dk$ and $|z|^2 := z\bar{z}$ for every quaternion $z \in \mathbb{H}$. Show that $|z_1 z_2| = |z_1|\,|z_2|$ for every pair of quaternions $z_{1/2} \in \mathbb{H}$.

c. Conclude that $\mathbb{H} \setminus \{0\}$ is a group under multiplication. (What is the inverse? Therefore $\mathbb{H}$ is called a division algebra.)