Abstract Algebra – II Groups (群理论)

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

October 12, 2012

Outline

Literature

P. Grillet: *Abstract algebra*, *Graduate texts in mathematics* (Springer, **2007**), ISBN 9780387715674, summary: melchiorG.freehosting.com/algebra → summary.

Definition

Definition (定义)

A group (群) *is a set (集合) G together with a binary operation $\cdot\colon G \times G \to G$ subject to the rules:*

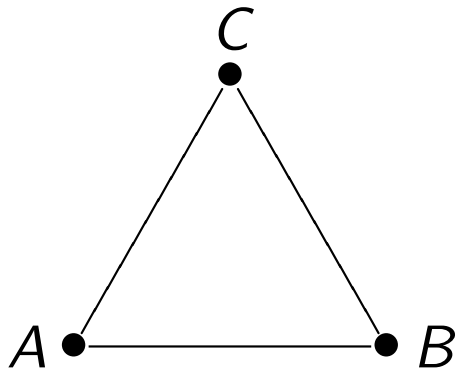
$$\forall a, b, c \in G\colon a(bc) = (ab)c, \tag{1}$$

$$\exists \mathrm{id} \in G\colon \forall a \in G\colon a\mathrm{id} = a = \mathrm{id}a, \tag{2}$$

$$\forall a \in G\colon \exists a^{-1} \in G\colon aa^{-1} = \mathrm{id} = a^{-1}a. \tag{3}$$

We define $(G : 1) := \operatorname{ord} G = |G|$ the cardinality of the group G. For finite groups this is the number of elements.

Example: symmetry group I



equilateral triangle (i.e. all 3 sides have the same length)

symmetry operations (对称操作):

- the identity (身份),
- 3 reflections (反思, on a straight line through each corner) τ_A, τ_B, and τ_C,
- and 2 rotations (回转) σ (counter-clockwise) and σ^{-1} (clockwise).

These are all symmetries, because a symmetry is uniquely determined by the image of the three corners A, B, C which can be permuted. The number of permutations is $3! = 6$ the above group elements.

Example: symmetry group II

group operation is composition:
$(\sigma \circ \tau_A)(B) := \sigma(\tau_A(B)) = \sigma(C) = A$, ..., $\sigma \circ \tau_A = \tau_C$.
Order is important: $\tau_A \circ \sigma = \tau_B \neq \tau_C = \sigma \circ \tau_A$
The multiplication table:

id	σ	σ^{-1}	τ_A	τ_B	τ_C
σ	σ^{-1}	id	τ_C	τ_A	τ_B
σ^{-1}	id	σ	τ_B	τ_C	τ_A
τ_A	τ_B	τ_C	id	σ	σ^{-1}
τ_B	τ_C	τ_A	σ^{-1}	id	σ
τ_C	τ_A	τ_B	σ	σ^{-1}	id

Associativity: any family of maps (from a space back to itself, called endomorphism, 自同态) $(f \circ g)(\Delta) := f(g(\Delta))$ and therefore $((f \circ g) \circ h)(\Delta) = (f \circ g)(h(\Delta)) = f(g(h(\Delta))) = f((g \circ h)(\Delta)) = (f \circ (g \circ h))(\Delta)$ where Δ ranges over all objects that can be

Example: symmetry group III

mapped. Therefore composition of endomorphisms is always associative.
Two observations: 1) every row contains every element exactly once (also every column contains every element exactly once).
2) in the upper left 3×3-corner there are only the elements id, σ, and σ^{-1} – this is called a subgroup.
This group is denoted D_3, because it is the symmetry groups of the equilateral triangle. Alternatively S_3, because it permutes the 3 corners.

Example: Numbers I

Consider the integers (整数) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ together with addition. The neutral element is obviously 0 (because $a + 0 = a = 0 + a$) and the inverse element to a is $-a$ (because $a + (-a) = 0 = (-a) + a$). Note that the group is infinite, but its operation is moreover commutative (交换), i.e. $b + a = a + b$. This group is denoted $(\mathbb{Z}, +)$.

Example: integers modulo n I

Remainders of dividing integers modulo (模) $n > 0$ are $\{0, 1, 2, \ldots, n-1\}$.
a and b have the same remainder iff $n|(b-a)$.
Arrange the integers in the classes (等价类)
$[0] = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$,
$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+2, \ldots\}$,
$[2] = \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}$, ...,
$[n-1] = \{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}$. We write

$$a \equiv b \pmod{n} \Leftrightarrow a - b = kn \text{ for some } k \in \mathbb{Z}.$$

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$, because $a - b = kn$ and $c - d = ln$ imply $(a + c) - (b + d) = (k + l)n$.

Example: integers modulo n II

Addition table mod n:

$[0]$	$[1]$	$[2]$	$[3]\ldots$	$[n-1]$
$[1]$	$[2]$	$[3]$	$[4]\ldots$	$[0]$
$[2]$	$[3]$	$[4]$	$[5]\ldots$	$[1]$
$\ldots$	$\ldots$			
$[n-1]$	$[0]$	$[1]$	$[2]\ldots$	$[n-2]$

This group is $(\mathbb{Z}/(n), +)$.

Example: Multiplication modulo p

Let $p = 7$ and consider multiplication modulo p.
$a \equiv b \pmod{p}$ and $c \equiv d \pmod{p}$ then $ac \equiv bd \pmod{p}$, because
$a - b = kp$ and $c - d = lp$ imply
$ac - bd = (a - b)c + b(c - d) = kpc + blp = (kc + bl)p$.
Multiplication with 0 gives 0, therefore not be an element of the multiplicative group (has no inverse).
The multiplication table:

$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

This group is denoted $(\mathbb{Z}/(p))^*$.

non-Examples

An example of an associative (联想, and commutative) operation that does not form a group: multiplication modulo 6

$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[4]$	$[0]$	$[2]$	$[4]$	$[0]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$
$[4]$	$[2]$	$[0]$	$[4]$	$[2]$	$[0]$
$[5]$	$[4]$	$[3]$	$[2]$	$[1]$	$[0]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$

no group, because e.g. $[2]$ has no inverse.
However $(\mathbb{Z}/(6))^* = \{[1], [5]\} \cong C_2$ is a group with respect to multiplication.
Q: What is the difference between $p = 7$ and $n = 6$?

non-Examples

An example of an associative (联想, and commutative) operation that does not form a group: multiplication modulo 6

$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[4]$	$[0]$	$[2]$	$[4]$	$[0]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$
$[4]$	$[2]$	$[0]$	$[4]$	$[2]$	$[0]$
$[5]$	$[4]$	$[3]$	$[2]$	$[1]$	$[0]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$

no group, because e.g. $[2]$ has no inverse.
However $(\mathbb{Z}/(6))^* = \{[1], [5]\} \cong C_2$ is a group with respect to multiplication.
Q: What is the difference between $p = 7$ and $n = 6$?
a: p is a prime while n is not.

Associativity test I

Most time-consuming, but necessary; Light-test:

id	σ	σ^{-1}	$\boldsymbol{\tau_A}$	τ_B	τ_C
σ	σ^{-1}	id	$\boldsymbol{\tau_C}$	τ_A	τ_B
σ^{-1}	id	σ	$\boldsymbol{\tau_B}$	τ_C	τ_A
$\rightarrow \tau_A$	τ_B	τ_C	$\mathbf{id}$	σ	σ^{-1}
$\Rightarrow \tau_B$	τ_C	τ_A	$\boldsymbol{\sigma^{-1}}$	id	σ
τ_C	τ_A	τ_B	$\boldsymbol{\sigma}$	σ^{-1}	id

$\rightarrow (\tau_A)$	τ_B	τ_C	id	σ	σ^{-1}
$\boldsymbol{\tau_C}$	.	.	σ	.	.
$\Rightarrow \boldsymbol{\tau_B}$	τ_C	τ_A	$\sigma^{-1} = \sigma^{-1}$	id	σ
$\mathbf{id}$	.	.	τ_A	.	.
$\boldsymbol{\sigma^{-1}}$	.	.	τ_B	.	.
$\boldsymbol{\sigma}$	.	.	τ_C	.	.

Table for $\tau_A \in S_3$.

Associativity test II

Lemma (引理)

Given a set X together with a binary operation $\cdot$. Let further X be generated (产生) by $S \subset X$ under the operation. If every element of S passes Light's test, then $\cdot$ is associative. □

Semigroups and monoids I

Definition

Given a set X together with a binary operation $\cdot : X \times X \to X$, we say that $(X, \cdot)$ is a semigroup *(半群) iff $\cdot$ is associative. If $\cdot$ has in addition a neutral element, we say that $(X, \cdot)$ is a* monoid *(幺半群). A (semi)-group is called* commutative / abelian *(可交换的) iff*

$$ba = ab \quad \forall a, b \in X.$$

Note that in a semi-group the inverse element is unique (独特), because $ea = a = ae$ and $e'a = a = ae'$ for all $a \in X$ imply $e = ee' = e'$. Also the inverse element is unique (if it exists), because $ai = e = ia$ and $aj = e = ja$ for some $a \in X$ imply $j = iaj = i$. A bit more interesting question is how much we can weaken the group axioms, i.e. do we really need that the inverse element is inverse from both sides?

Semigroups and monoids II

Consider therefore the set of all sequences (序列) Seq $:= \mathbb{R}^{\infty}$ together with the operation $T : \text{Seq} \to \text{Seq} : (a_n) \mapsto (0, a_{n-1})$, i.e. the sequence is shifted to the right by inserting a leading 0. Obviously the operation $S : \text{Seq} \to \text{Seq} : (a_n) \mapsto (a_{n+1})$ that shifts sequences to the left (and drops the first element) fulfills $ST = \mathrm{id}$, but on the other hand $TS : \text{Seq} \to \text{Seq} : (a_n) \mapsto (0, a_n)$ is not the identity, but sets the first element of the sequence to 0.

Dihedral groups I

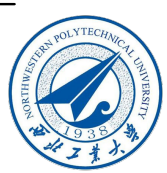
The example with the equilateral triangle has the following generalization:

Definition

The dihedral group (二面体群) D_n is the symmetry group of the regular n-gon in the plane.

Example

3. $D_3 = \{\mathrm{id}, \sigma, \sigma^{-1}, \tau_A, \tau_B, \tau_C\}$.
4. $D_4 = \{\mathrm{id}, \tau, \tau^2, \tau^{-1}, \sigma_A, \sigma_a, \sigma_B, \sigma_b\}$ where τ is a rotation by 90^o, σ_A the reflection on the diagonal AC, and σ_a the reflection on the perpendicular bisector of a (and of c).
n. $D_n = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}, \sigma, \sigma\tau, \ldots, \sigma\tau^{n-1} : \tau^k\tau^l = \tau^{k+l}, \sigma^2 = \mathrm{id}, \sigma\tau^k\sigma = \tau^{-k}, \tau^k\sigma\tau^l = \sigma\tau^{-k+l}\}$



Exercises I

Exercise

Given a semi-group $(X, \cdot)$ with a left-neutral element (i.e. $e \in X$ such that for all $a \in X$: $ea = a$) and left-inverses (for all $a \in X$ there is an $a_L \in X$ such that $a_L a = e$), show that $(X, \cdot)$ is a group. What happens when we require a right-neutral and right-inverse elements?

Exercise

Let $(X, \cdot)$ be a semi-group and assume for every $a, b \in X$ the equations $ax = b$ and $ya = b$ have a solution. Show that $(X, \cdot)$ is a group.

Exercise

Exercises II

Let $(X, \cdot)$ be a finite semi-group. Assume that for every $a \in X$ the cancellation law (取消法则) holds, i.e. $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$. Show that $(X, \cdot)$ is a group.
Given an example of an infinite semigroup where the cancellation law holds, but that is not a group.

Exercise

Describe the group of symmetries of the sine curve ($y = \sin x$ over the real numbers, 实数), i.e. list all its elements and write a multiplication table (compactly).

Exercise

Exercises III

Given a group $(G, \cdot)$. Show that $a^m a^n = a^{m+n}$ for all $a \in G$ and $m, n \in \mathbb{Z}$ where a^m has the usual meaning, i.e. $a^m = \underbrace{aa \cdots a}_{m \text{ times}}$ for $m > 0$, $a^0 = \mathrm{id}$ and $a^{-m} = (a^m)^{-1}$. Show moreover $(a^m)^n = a^{mn}$ for the same elements.

Exercise

Show that a finite group with an even number of elements contains an even number of elements x such that $x^{-1} = x$.
State and prove a similar statement for finite groups with an odd number of elements.

Subgroups (子群)

Definition

Given a group $(G, \circ)$*, then a subset* $H \subset G$ *containing the neutral element* $\mathrm{id} \in H$ *and all inverse* $h^{-1} \in H$ *of its elements* $h \in H$ *that is closed under the operation* $H \circ H \subset H$ *is called a subgroup (子群).*

We denote $\langle g \rangle \subset G$ *the subgroup generated by (所产生)* $g \in G$ *and more generally* $\langle S \rangle \subset G$ *the smallest subgroup containing the subset* $S \subset G$*.*

We denote $\operatorname{ord} g := (\langle g \rangle : 1)$ *the order of an element* $g \in G$*.*

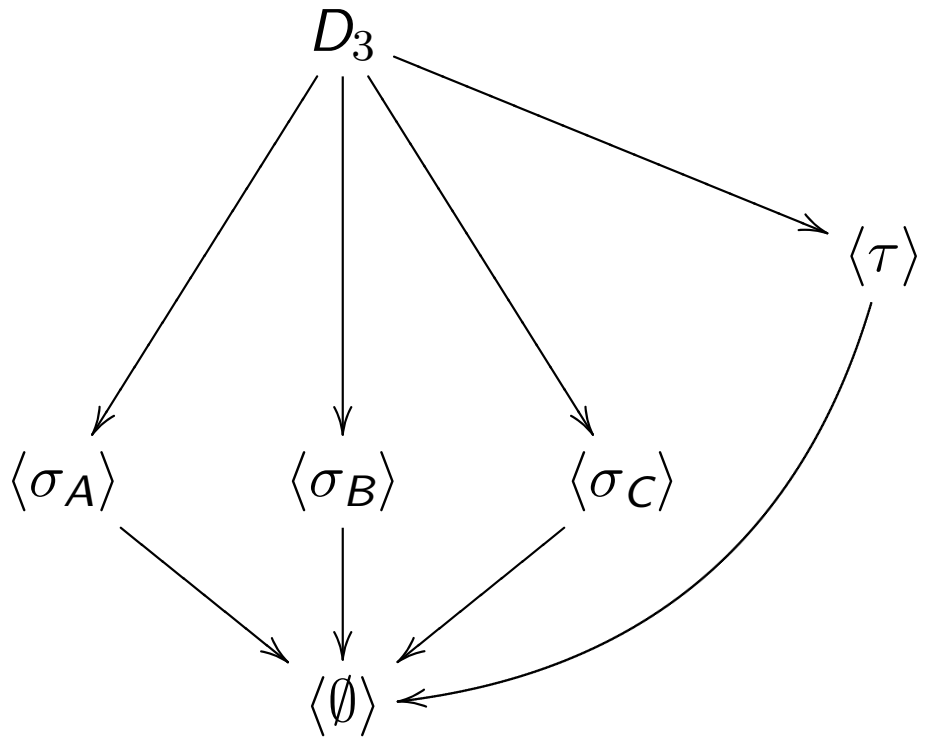
We call a group $(G, \cdot)$ cyclic *(循环) iff there is an element* $g \in G$ *such that* $G = \langle g \rangle$*.*

Subgroup Examples

Example

0. The standard examples are $(\mathbb{Z},+) \subset (\mathbb{Q},+) \subset (\mathbb{R},+) \subset (\mathbb{C},+)$ as well as $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.
1. Consider the group $(\mathbb{Z},+)$. We can start from an element $n \in \mathbb{Z}$ to form the subgroup generated by n as $\langle n \rangle_{\mathbb{Z}} = n\mathbb{Z}$. Conversely given a finite number of elements $\{n_1, \ldots, n_k\}$ then the subgroup generated by them is the group $d\mathbb{Z}$ where $d = \gcd(n_1, \ldots, n_k)$ is the greatest common divisor. Therefore all subgroups of $\mathbb{Z}$ are cyclic.
2. Consider the group $D_3 = \{\mathrm{id}, \sigma_A, \sigma_B, \sigma_C, \tau, \tau^{-1}\}$. Its subgroups are $\{\mathrm{id}\} = \langle \emptyset \rangle$, $\{\mathrm{id}, \sigma_A\} = \langle \sigma_A \rangle$, $\langle \sigma_B \rangle$, $\langle \sigma_C \rangle$, $\langle \tau \rangle$, and D_3. These fit into the following scheme (子群方案)

Subgroup Examples II



Subgroup condition

Proposition (命题)

Given a group $(G, \cdot)$ then a non-empty subset $H \subset G$ is a subgroup iff for all $x, y \in H$ also $xy^{-1} \in H$.

Proof.

Since there is an $h \in H$, $\mathrm{id} = hh^{-1} \in H$. But then also $h^{-1} = \mathrm{id}h^{-1} \in H$. □

Proposition

Given a finite *(有限) group $(G, \circ)$, then a non-empty subset $H \subset G$ is a subgroup iff for all $x, y \in H$ also $xy \in H$.*

As the example of the natural numbers $\mathbb{N} \subset \mathbb{Z}$ shows, the assumption finite is important.

Subgroup condition II

Proof.

We want to use the previous proposition, but first need to show that for every $h \in H$ also $h^{-1} \in H$. We consider the subset $\langle h \rangle_+ := \{h^n : n \in \mathbb{N}_+\} \subset H$. Since G is finite, also H and thus $\langle h \rangle_+$ is finite. Therefore there are $m - 1 > n \in \mathbb{N}_+$ such that $h^m = h^n$. Since there is $h^{-1} \in G$. we conclude that $h^{m-n} = \mathrm{id} \in H$. But then also $h^{-1} = h^{m-n-1} \in H$ which completes the proof. □

Union of subgroups

Union (并集) of subgroups generally does not lead to a subgroup, e.g. $h_i \in H_i \subset G$ but $h_2 \notin H_1$ and $h_1 \notin H_2$, then $h_1 h_2 \notin H_1 \cup H_2$.
However in the following special case it does.

Proposition

Given a group $(G, \cdot)$ and an ascending chain of subgroups $H_0 \subset H_1 \subset H_2 \subset \cdots \subset G$, then their union $\bigcup_{n\geq 0} H_n$ is a subgroup of G.

interesting of course when the chain is infinite.

Proof.

$H_\infty := \bigcup_{n\geq 0} H_n$. $\mathrm{id} \in H_0 \subset H_\infty$. Let $g \in H_\infty$. Then there is a (finite) number $m \in \mathbb{N}$ such that $g \in H_m$. Then also $g^{-1} \in H_m \subset H_\infty$, because H_m is a group. Let finally $g, h \in H_\infty$. Then there are (finite) numbers $m, n \in \mathbb{N}$ such that $g \in H_m$ and $h \in H_n$. Let $M = \max(m, n)$ be their maximum, then also $g, h \in H_M$ and thus $gh \in H_M \subset H_\infty$. □

Homework: Prove that the intersection (交集) of subgroups always is a subgroup.

Cosets (左陪集)

Definition

Given a subgroup $H \subset G$ of a group, we define its left-cosets (左陪集) as $G/H := \{gH : g \in G\}$. The set of right-cosets (右∼) is $H\backslash G := \{Hg : g \in G\}$.

For abelian groups the two notions coincide, however in general they can be different.

Proposition (Lagrange's theorem, 拉格朗日定理)

Given a subgroup $H \subset G$ then its left-cosets (right-cosets) are disjoint. Moreover all cosets have the same cardinality as H. For G finite we have ord $H|$ ord G *and in particular that the number of left-cosets equals the number of right-cosets. Also the order of every element $g \in G$ divides the group order* ord $g|$ ord G.

Cosets (左陪集) II

Proof.

The bijection $G \to G : g \mapsto g^{-1}$ with $gh \mapsto h^{-1}g^{-1}$ maps $Hg \to g^{-1}H$ right-cosets bijectively onto left-cosets. Thus sufficient to prove for left-cosets.

Given two cosets g_iH, $i = 1, 2$ whose intersection $g \in g_1H \cap g_2H$ is nonempty. Then there exist $h_i \in H$ such that $g = g_ih_i$. Therefore also $gh_i^{-1} = g_i$ and so $g_1H = gH = g_2H$.

For the second statement note that $g_1 = gh_1 = gh_2$ (with $h_{1/2} \in H$) implies by multiplication with g^{-1} from the left that $h_1 = h_2$. Therefore the map $H \to gH : h \mapsto gh$ is injective and surjective from H to the orbit gH for every $g \in G$.

In the last statement we just count $\operatorname{ord} G = |G/H| \operatorname{ord} H$. This completes the proof. □

We denote $[G : H] := |G/H|$ the index of H in G.

Cosets (左陪集) III

Remark

The relation $g \sim g'$ iff $gH = g'H$ is an equivalence relation (等价关系), i.e. $g \sim g$, $g \sim g' \Rightarrow g' \sim g$, and $g \sim g' \wedge g' \sim g'' \Rightarrow g \sim g''$ for all $g, g', g'' \in G$. Every equivalence relation breaks a set into disjoint equivalence classes.

Example

Let $G = D_3$ and $H = \langle \sigma_A \rangle$. The equivalence classes G/H are $\{H = \{\mathrm{id}, \sigma_A\}, \sigma_B H = \{\sigma_B, \tau^{-1}\}, \sigma_C H = \{\sigma_C, \tau\}\}$ i.e. there are $3!/2 = 3$ equivalence classes. Note that the set G/H does not have any induced group structure, e.g. $H\sigma_B H$ has 4 elements.

Group homomorphisms (群同态) I

Definition

Given two groups G and H. A group homomorphism (群同态) is a map $\phi\colon G \to H$ such that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$, $\forall g_i \in G$.
We denote $\operatorname{im}\phi = \{\phi(g) : g \in G\}$ *the* image *(图像) of ϕ*
and $\ker\phi := \{g \in G : \phi(g) = \mathrm{id}\}$ *the* kernel *(内核) of ϕ.*
A group homomorphism $\phi\colon G \to H$ is called
injective (monomorphism, 单同态) *if* $\ker\phi = \{\mathrm{id}\}$, *it is called*
surjective (epimorphism, 满同态) *if* $\operatorname{im}\phi = H$. *It is called*
bijective (isomorphism, 双同态) *if it is injective and surjective.*
If there is a group isomorphism $\phi\colon G \to H$, we call G and H isomorphic, denoted as $G \cong H$.

Note that the composition of group homomorphisms $\phi\colon H \to K$ and $\psi\colon G \to H$ is $\phi \circ \psi\colon G \to K : g \mapsto \phi(\psi(g))$ and is a group

Group homomorphisms (群同态) II

homomorphism, because
$(\phi \circ \psi)(g_1 g_2) = \phi(\psi(g_1)\psi(g_2)) = (\phi \circ \psi)(g_1) \cdot (\phi \circ \psi)(g_2)$.
Also note that for a group homomorphism $\phi\colon G \to H$,
$\phi(\mathrm{id}_G) = \mathrm{id}_H$, $\phi(g^{-1}) = (\phi(g))^{-1}$ and $\phi(g^n) = (\phi(g))^n$.

Example

0. Let G and H be any groups and $\mathrm{id}_H \in H$ the identity of H. Then $\phi_0\colon G \to H : g \mapsto \mathrm{id}_H$ is a (rather trivial) group homomorphism.
   Another example of a group homomorphism is the identity: $\mathrm{Id}_G\colon G \to G : g \mapsto g$.
1. A non-trivial example would be e.g. $e\colon (\mathbb{Z}, +) \to (\mathbb{R}, +)$ a monomorphism (also called an embedding, 包埋).

Mapping behavior of homomorphisms

Proposition

Given a subgroup $H \subset G$, then the image under a group homomorphism $\phi\colon G \to G'$ is also a subgroup $\phi(H) \subset G'$. Conversely, for $J \subset G'$ also $\phi^{-1}(J) := \{g \in G : \phi(g) \in J\}$ is a subgroup.

Proof.

First case: $g_{1/2} \in \phi(H)$ imply $h_{1/2} \in H$ with $\phi(h_i) = g_i$. Then $h_1 h_2 \in H$ and so $\phi(h_1 h_2) = \phi(h_1)\phi(h_2) = g_1 g_2$. For $g_1 \in \phi(H)$, $\phi(h_1^{-1}) = ((\phi(h_1))^{-1} = g_1^{-1} \in \phi(H)$ and $\mathrm{id}' = \phi(\mathrm{id}) \in \phi(H)$.
Second case: $g_{1/2} \in \phi^{-1}(J)$ implies $\phi(g_i) \in J$ and thus $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \in J$, i.e. $g_1 g_2 \in \phi^{-1}(J)$. Further $\phi(\mathrm{id}) = \mathrm{id}' \in J$ and so $\mathrm{id} \in \phi^{-1}(J)$. Finally $\phi(g^{-1}) = (\phi(g))^{-1} \in J$ and therefore $g^{-1} \in \phi^{-1}(J)$ for every $g \in \phi^{-1}(J)$. □

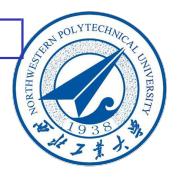
Mapping behavior of homomorphisms II

Corollary (推论)

Given a group homomorphism $\phi\colon G \to H$*, then* $\operatorname{im}\phi \subset H$ *and* $\ker\phi \subset G$ *are subgroups. Moreover the left-cosets* $G/\ker\phi$ *coincide with the right-cosets* $\ker\phi\backslash G$*, i.e.* $g\ker\phi = (\ker\phi)g$ *for all* $g \in G$*.*

Proof.

The first statement follows immediately from the last proposition when you notice that $\operatorname{im}\phi = \phi(G)$ and $\ker\phi = \phi^{-1}(\mathrm{id})$ which are both trivial subgroups.
Finally $g\ker\phi \subset \phi^{-1}(h)$ for $h = \phi(g)$, because $\phi(g\ker\phi) = \phi(g)\phi(\ker\phi)$. Conversely $\phi(g') = h = \phi(g)$, then $\phi(g^{-1}g') = \mathrm{id}_H$ and so $g^{-1}g' = g_0 \in \ker\phi$, i.e. $g' = gg_0 \in g\ker\phi$.
Analogously $(\ker\phi)\cdot g = \phi^{-1}(h)$.



Normal subgroups (正规子群)

Definition

A subgroup $H \subset G$ is called normal subgroup *(正规子群) if the left-cosets coincide with the right-cosets, i.e. for all $g \in G$, $gH = Hg$.*

Note that a subgroup $N \subset G$ is normal iff $gNg^{-1} \subset N$ for all $g \in G$.

Example

Consider the group $S_3 = D_3$ and the map
$\operatorname{sgn}\colon S_3 \to (\{\pm 1\}, \cdot) : \{\mathrm{id}, \tau, \tau^{-1}\} \to \{1\}, \{\sigma_A, \sigma_B, \sigma_C\} \to \{-1\}$.
As we can check, this gives a group homomorphism, i.e.
$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$ for all $\alpha, \beta \in S_3$. $\operatorname{im}(\operatorname{sgn}) = H := \{\pm 1\}$.
kernel is $A_3 := \ker \operatorname{sgn} = \{\mathrm{id}, \tau, \tau^{-1}\} \lhd S_3$ which is therefore a normal subgroup.

Normal subgroups (正规子群) II

Proposition

Given a normal subgroup $N \triangleleft G$, then the set of cosets inherits a group structure together with the surjective group homomorphism $\pi : G \to G/N : g \mapsto gN$ called quotient map.

Proof.

We want to define the group operation by representatives, i.e.

$$(gN)(hN) := (gh)N, \tag{4}$$

but for this we need to check that this is representative independent (代表性的独立). This is easy to see, because $Nh = hN$ by the preliminaries and thus $(gN)(hN) = gNhN = ghNN = ghN$, i.e. the coset multiplication is indeed the elementwise multiplication of the cosets, but this is independent of the representatives g_i of the coset g_iN as well as for h_i and h_iN. Now it follows that π is a group homomorphism.
Finally surjectivity of the map π follows from the definition of G/N. □

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

Exercise

Given a group G and a family of subgroups $\{S_\alpha \subset G : \alpha \in A\}$. Show that

a. The intersection $\bigcap_{\alpha \in A} S_\alpha$ is a subgroup;

b. if all $S_\alpha \triangleleft G$ are normal, then the intersection is also normal.

Exercise

Let $G = D_n$ and $H = \{\mathrm{id}, \tau\}$. Show that for $n \geq 3$ the partition into left-cosets is different from the partition into right-cosets.

Exercises II

Exercise

a. Give a group together with two subgroups whose union is not a subgroup.

b. Given a group G together with two subgroups $S_{1/2} \subset G$. Show that $S_1 \cup S_2$ is a subgroup iff $S_1 \subset S_2$ or $S_2 \subset S_1$.

Exercise

Show that every group of prime order is simple (i.e. has only trivial subgroups) and cyclic.

Exercise*

Given a finite group G. A subgroup $M \subset G$ is called maximal iff it is different from G ($M \neq G$) and there is no subgroup properly in between ($M \subsetneq S \subsetneq G$). Show that every subgroup $H \subsetneq G$ that does not coincide with G is contained in a maximal subgroup.

Exercises III

Exercise

Given a group G together with two subgroups $H, K \subset G$. Show that the intersection of a left-coset of H with a left-coset of K is either empty or a left-coset of $H \cap K$.

Exercise

Given a group isomorphism $\phi\colon G \to H$ show that its inverse $\phi^{-1}\colon H \to G : \phi(g) \mapsto g$ is also a group homomorphism.

Exercises IV

Exercise

Given a group homomorphism $\phi\colon G \to H$.

a. Assume that $N \triangleleft H$ is a normal subgroup. Show that $\phi^{-1}(N) \triangleleft G$ is a normal subgroup.
b. Assume that ϕ is surjective and $N \triangleleft G$ is a normal subgroup of G. Show that $\phi(N) \triangleleft H$ is a normal subgroup.
c. Find an example of a group homomorphism and a normal subgroup such that the image of the normal subgroup is not normal.

Exercise

Show that D_4 contains subgroups $A \subset N \subset D_4$ such that $A \triangleleft N$ and $N \triangleleft D_4$, but not $A \triangleleft D_4$.

Exercise

Prove that every subgroup of index 2 is normal.

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.