Group Theory – Problem Sheet 1

Exercise sheet 1, Group Theory, Prof. Daniel Roggenkamp

Solutions by Janosh Riebesell, 12.05.2015

Exercise 1 (Definitions)

a) Define what a group is and show from the axioms that left-identity and -inverses are also right-identity and -inverses, and that identity and inverses are unique.

Group: algebraic structure $(G, \langle\cdot,\cdot\rangle)$ consisting of
- a set of elements G and
- an operation $\langle\cdot,\cdot\rangle$ that satisfies the group axioms:

1. Closure: $\forall a, b \in G : \langle a, b\rangle \in G$
2. Associativity: $\forall a, b, c \in G : \langle\langle a, b\rangle, c\rangle = \langle a, \langle b, c\rangle\rangle$
3. Identity: $\exists! e \in G\, \forall a \in G : \langle e, a\rangle = a$
4. Inverse: $\forall a \in G\, \exists! a^{-1} \in G : \langle a^{-1}, a\rangle = e$

From now on, the group operation between two elements of a group is implicit, i.e. $\langle a, b\rangle \to ab$. We prove that left- and right-identity and inverse are equal and their uniqueness:

$$a^{-1}a = e \implies a^{-1}(aa^{-1}) = \underbrace{(a^{-1}a)}_{e}a^{-1} = ea^{-1} = a^{-1} \qquad \implies aa^{-1} = e \quad \text{(right inverse)},$$

$$aa^{-1} = e \implies ae = a(a^{-1}a) = \underbrace{(aa^{-1})}_{e}a = ea \qquad \implies ae = a \overset{!}{=} ea \quad \text{(right identity)},$$

$$\text{assume } \exists e, e' \in G : ea = a, e'a = a\, \forall a \in G \implies e = ee' = e' \qquad \implies e = e' \quad \text{(identity unique)},$$

$$\text{assume } \exists a^{-1}, a'' \in G : a^{-1}a = e, a''a = e\, \forall a \in G \implies a^{-1}a = e = a''a \implies a^{-1} = a'' \quad \text{(inverse unique)}.$$

b) What is a group homomorphism? Show that the map $\mathbb{Z} \to \mathbb{Z}_n$, $z \mapsto [z]$ is a group homomorphism.

Group homomorphism: given two groups $(G, *)$, $(H, \cdot)$, $\varphi : G \to H$ is a group homomorphism if

$$\varphi(g_1 * g_2) = \varphi(g_1) \cdot \varphi(g_2) \quad \forall g_1, g_2 \in G.$$

Here:

$$\forall z_1, z_2 \in \mathbb{Z} : \quad [z_1 + z_2] = [z_1] + [z_2].$$

c) What is a subgroup? Show that the rotations form a subgroup $\mathbb{Z}_n \subset D_n$ of the dihedral group D_n.

Given a group $(H, \cdot)$, a subset $G \subset H$ is a subgroup if $(G, \cdot)$ is itself a group under the operation of H, i.e. G contains e and is closed under multiplication and inversion.

$$D_n = \{R_0, R_1, ..., R_{n-1}, S_0, S_1, ..., S_{n-1}\},$$

the group of symmetries of a regular n-gon,

$$\mathbb{Z}_n = D_n \setminus \{S_0, S_1, ..., S_{n-1}\} = \{R_0, ..., R_{n-1}\} \subset D_n$$

is a subgroup: it contains $e = R_0$, is closed since $R_i R_j = R_{i+j \bmod n}$, and contains the inverses $R_i^{-1} = R_{n-i \bmod n}$.

d) What are conjugacy classes? Determine all conjugacy classes of D_4 and D_5. What about general D_n?

Conjugacy class:

$$C_g = [g] = \{g' \in G \mid \exists \tilde{g} \in G : \tilde{g} g \tilde{g}^{-1} = g'\},$$

$$D_4 = \{R_0, R_1, R_2, R_3, S_0, S_1, S_2, S_3\} : \quad \{R_0\}, \quad \{R_2\}, \quad \{R_1, R_3\}, \quad \{S_0, S_2\}, \quad \{S_1, S_3\},$$
$$D_5 = \{R_0, ..., R_4, S_0, ..., S_4\} : \quad \{R_0\}, \quad \{R_1, R_4\}, \quad \{R_2, R_3\}, \quad \{S_0, S_1, S_2, S_3, S_4\}.$$

In general, conjugation by a rotation leaves rotations invariant and shifts reflections by two, $R_j S_i R_j^{-1} = S_{i+2j}$, while conjugation by a reflection inverts rotations, $S_j R_i S_j^{-1} = R_{-i}$. Hence the classes of D_n are $\{R_0\}$ and the pairs $\{R_i, R_{-i}\}$, plus for odd n a single class of all reflections, and for even n the additional class $\left\{R_{n/2}\right\}$ and two classes of reflections, $\{S_0, S_2, ...\}$ and $\{S_1, S_3, ...\}$.

Exercise 2 (Finite groups)

a) Let G be a finite group with a prime number of elements. What can you say about G?

By Lagrange's theorem, G can only have the two trivial subgroups $\{e\}$ and G. Since we can always construct orbits Γ_g for all elements $g \in G$, which by the closure axiom are subgroups of G, we have $\Gamma_e = \{e\}$ or $\Gamma_g = G$. Since Γ_g is isomorphic to $\mathbb{Z}_{|G|}$, $\Gamma_g \cong \mathbb{Z}_{|G|}$, we have that G is isomorphic to $\mathbb{Z}_{|G|}$, $G \cong \mathbb{Z}_{|G|}$.

b) Write the multiplication table of $\mathbb{Z}_3$ and the respective embedding $\mathbb{Z}_3 \hookrightarrow S_3$ into the symmetric group.

$\mathbb{Z}_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$\mathbb{Z}_3 \overset{\pi}{\hookrightarrow} S_3:$$

$$\pi_0 : 0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix},$$
$$\pi_1 : 1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix},$$
$$\pi_2 : 2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

Exercise 3 (Symmetric group)

a) Write the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 2 & 4 & 6 \end{pmatrix}$ as product of non-intersecting cycles.

$$\pi = (1\,3\,5\,4\,2)(6)$$

b) What is the order of S_3? How many conjugacy classes does S_3 have? Determine their sizes, and give a representation of each one.

$|S_3| = 3! = 6$. S_3 has $p(3) = 3$ conjugacy classes, where $p(n)$ is the number of partitions of n. Conjugacy class sizes can be calculated using

$$|C_{(k_1,\dots,k_n)}| = \frac{n!}{\prod_i i^{k_i} k_i!},$$

where the k_i give the number of permutation cycles of length i. Considering the different partitions of n, we get

$$\begin{aligned}
\lambda = (3,0,0), \quad k = (3,0,0): \quad C_{(3,0,0)} &= \frac{3!}{1^3 3! \cdot 2^0 0! \cdot 3^0 0!} = 1, \\
\lambda = (2,1,0), \quad k = (1,1,0): \quad C_{(1,1,0)} &= \frac{3!}{1^1 1! \cdot 2^1 1! \cdot 3^0 0!} = 3, \\
\lambda = (1,1,1), \quad k = (0,0,1): \quad C_{(0,0,1)} &= \frac{3!}{1^0 0! \cdot 2^0 0! \cdot 3^1 1!} = 2.
\end{aligned}$$

Representatives:

$$\begin{aligned}
\lambda = (3,0,0): &\quad e = (1)(2)(3), \\
\lambda = (2,1,0): &\quad (1\,2)(3), \\
\lambda = (1,1,1): &\quad (1\,2\,3).
\end{aligned}$$

c) Show that $H = \{e, (1,2)\} \subset S_3$ is a subgroup. Is it normal?

Closure of H:

$$ee = e \in H, \quad e(1,2) = (1,2) \in H, \quad (1,2)e = (1,2) \in H,$$
$$(1,2)(1,2) = e \in H.$$

Associativity: is inherited from S_3, since $e, (1,2) \in S_3$.

Identity: e ✓

Inverse: $ee = e$, $(1,2)(1,2) = e$ ✓

All four group axioms are met. Therefore $H \subset S_3$ is a subgroup. Since H cannot be formed by conjugacy classes of S_3, it is not normal in S_3.

Exercise 4 (Commutator subgroup)

Let G be a group. The commutator of two elements $g, h \in G$ is defined by $[g,h] \coloneqq g^{-1}h^{-1}gh \in G$. The commutator subgroup of G is the group generated by all commutators in G:

$$[G,G] = \{[g_1,h_1]\cdots[g_n,h_n] \mid n \in \mathbb{N}, g_i, h_i \in G\}.$$

a) Show that the commutator subgroup is indeed a subgroup $[G,G] \subset G$.

We use the condition that if for all $[g,h],[k,l] \in [G,G]$, $[g,h][k,l]^{-1} \in [G,G]$, where $g,h,k,l \in G$, then $[G,G] \subset G$ is a subgroup. We have

$$[k,l]^{-1} = \left(k^{-1}l^{-1}kl\right)^{-1} = l^{-1}k^{-1}lk = [l,k]$$

and therefore

$$[g,h][k,l]^{-1} = [g,h][l,k] \in [G,G]$$

by definition of $[G,G]$.

b) Show that it is a normal subgroup $[G, G] \lhd G$.

$$[G, G] \lhd G \text{ is a normal subgroup} \iff \forall g \in G : g[G, G]g^{-1} = [G, G].$$

We prove the above equality by showing that each is a subgroup of the other.

$g[G, G]g^{-1} \subset [G, G]$: $\forall g \in G$, $[k, l] \in [G, G]$, we have

$$[k, l]^{-1} g[k, l]g^{-1} = [[k, l], g^{-1}] \in [G, G].$$

From this it follows, since $[G, G] \subset G$ is a subgroup fulfilling closure w.r.t. the group action, that

$$[k, l][k, l]^{-1} g[k, l]g^{-1} = g[k, l]g^{-1} \in [G, G].$$

$g[G, G]g^{-1} \supset [G, G]$: $\forall [k, l] \in [G, G]$ $\exists m, n \in G$: $gmg^{-1} = k \wedge gng^{-1} = l$, where we used that conjugation is a homomorphism on G

$$\begin{aligned} \implies [k, l] &= [gmg^{-1}, gng^{-1}] = (gmg^{-1})^{-1}(gng^{-1})^{-1} gmg^{-1}gng^{-1} \\ &= gm^{-1}g^{-1}gn^{-1}g^{-1}gmg^{-1}gng^{-1} = gm^{-1}n^{-1}mng^{-1} \\ &= g[m, n]g^{-1} \in g[G, G]g^{-1}. \end{aligned}$$

Therefore, $[G, G] \lhd G$.

Exercise 5 (Group actions)

An action of a group G on a set X is a group homomorphism $\varphi : G \to \mathrm{Bij}(X)$ from G into the group $\mathrm{Bij}(X)$ of bijections from X to X. One often uses the abbreviated notation $gx := \varphi(g)(x)$. For any $x \in X$ its orbit in G is defined by

$$\mathrm{Orb}_G(x) = Gx = \{gx \mid g \in G\} \subset X.$$

The stabilizer of $x \in X$ is defined by

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \subset G.$$

a) Show that the stabilizer is a subgroup of G.

For this, we again resort to the 'one-step' subgroup test, i.e. we show that $\mathrm{Stab}_G(x) \subset G$ is a *subset* of G and that $\mathrm{Stab}_G(x) \neq \varnothing$ is not empty (both of which are fulfilled by definition) and that $\forall a, b \in \mathrm{Stab}_G(x)$, we have $ab^{-1} \in \mathrm{Stab}_G(x)$, where always $x \in X$. For such a and b, we can write

$$\begin{aligned} b^{-1}x = b^{-1}(bx) &\overset{!}{=} (b^{-1}b)x = x, \quad \text{where we used that } \varphi \text{ is a homomorphism,} \\ \implies (ab^{-1})x &= a(b^{-1}x) = ax = x \\ \implies ab^{-1} &\in \mathrm{Stab}_G(x) \quad \text{and} \quad \mathrm{Stab}_G(x) \subset G. \end{aligned}$$

b) Show that stabilizers of elements $y, y' \in X$ which lie in the same G-orbit (i.e. $y, y' \in \mathrm{Orb}_G(x)$ for some $x \in X$) are conjugate.

Since $y, y' \in \mathrm{Orb}_G(x)$, $\exists a, b \in G : ax = y, bx = y'$. G being a group, we can invert to get $a^{-1}y = x = b^{-1}y'$. For any $g \in \mathrm{Stab}_G(y)$, we have

$$gy = y \iff g(ax) = ax \iff a^{-1}g(ax) = x.$$

Inserting $x = b^{-1}y'$ gives

$$a^{-1}g(ab^{-1}y') = b^{-1}y' \quad \Longleftrightarrow \quad (ba^{-1})g(ab^{-1})y' = y',$$

from which we deduce that

$$\underbrace{(ba^{-1})}_{h} g \underbrace{(ab^{-1})}_{h^{-1}} =: hgh^{-1} \in \mathrm{Stab}_G(y').$$

Since this holds for all $g \in \mathrm{Stab}_G(y)$, we found $h\,\mathrm{Stab}_G(y)\,h^{-1} = \mathrm{Stab}_G(y')$.

c) Show that the map $Gx \to G/\mathrm{Stab}_G(x)$, which sends $gx \mapsto g\,\mathrm{Stab}_G(x)$, is well defined (i.e. $gx = hx \Longrightarrow g\,\mathrm{Stab}_G(x) = h\,\mathrm{Stab}_G(x)$) and is a bijection.