Homework 1, Solutions

M. Gr. after [Gri07]

2012/10/14

1.1 Group definition

Exercise 1.1.1. 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?

Solution. First note that $aa_L = e_L a a_L = a_{LL}(a_L a)a_L = a_{LL}(e_L a_L) = a_{LL}a_L = e_L$ shows that a_L is also a right-inverse. Secondly note that $ae_L = (aa^{-1})a = e_L a = a$. This shows that e_L is the neutral element.

In the converse case note the anti-homomorphism ${}^T : (X, \cdot) \to (X, \cdot) : g_1 \cdots g_n \mapsto g_n \cdots g_1$ which maps $(gh)^T = h^T g^T$, but otherwise preserves the structure and thus reduces the right-neutral and right-inverse to a left-neutral and left-inverse. $\square$

Exercise 1.1.2. 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.

Solution. Let $a \in X$ be any element and $e_{aL} \in X$ the solution of $xa = a$. Then there is for every $b \in X$ a $b_L \in X$ such that $b_L b = e_{aL}$. But also a y such that $ay = b$. Therefore $e_{aL}b = e_{aL}ay = ay = b$. Thus e_{La} is a left-neutral element for the whole operation $\cdot$. Now the last exercise shows that $(X, \cdot)$ is a group. $\square$

Exercise 1.1.3.

a. Let $(X, \cdot)$ be a finite semi-group. Assume that for every $a \in X$ the cancellation law holds, i.e. $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$. Show that $(X, \cdot)$ is a group.

b. Given an example of an infinite semigroup where the cancellation law holds, but that is not a group.

Solution.

a. The cancellation laws show that $a\cdot\colon X \to X$ and $\cdot a\colon X \to X$ are injective. Because X is finite, this implies that they are also surjective. I.e. for every pair $a, b \in X$ there are $x, y \in X$ with $ax = b = ya$. Therefore the last exercise this shows that $(X, \cdot)$ is a group.

b. The example $(\mathbb{N}_+, +)$shows that the cancellation laws (which hold, because $(\mathbb{N}_+, +) \subset (\mathbb{Z}, +)$ is a semi-subgroup) alone are not enough.

□

Exercise 1.1.4. Describe the group of symmetries of the sine curve ($y = \sin x$ over the real numbers), i.e. list all its elements and write a multiplication table (compactly).

Solution. The known symmetry properties are sin is odd (point symmetry/ rotation ρ by 180°) and period length $p = 2\pi$ (translation symmetry τ). But we also know that sin is axial symmetric about $x = \pi/2$ (reflection symmetry σ). This gives the symmetry group $S = \langle \rho, \tau, \sigma \rangle \subset \mathrm{ISO}(\mathbb{R}^2)$ or as table:

id	τ^n	$\sigma\tau^n$	$\rho\tau^n$	$\sigma\rho\tau^n$
τ^m	τ^{m+n}	$\sigma\tau^{n-m}$	$\rho\tau^{n-m}$	$\sigma\rho\tau^{n+m}$
$\sigma\tau^m$	$\sigma\tau^{m+n}$	τ^{n-m}	$\sigma\rho\tau^{n-m}$	$\rho\tau^{n+m}$
$\rho\tau^m$	$\rho\tau^{m+n}$	$\sigma\rho\tau^{n-m-2}$	τ^{n-m}	$\sigma\tau^{n+m+2}$
$\sigma\rho\tau^m$	$\sigma\rho\tau^{m+n}$	$\rho\tau^{n-m-2}$	$\sigma\tau^{n-m}$	τ^{n+m+2}

Remark. We can thus write down the group compactly $S = \langle \tau, \sigma, \rho : \sigma^2 = \mathrm{id} = \rho^2, \rho\tau\rho = \tau^{-1}, \sigma\tau\sigma = \tau^{-1}, \sigma\rho\sigma = \rho\tau^{-2} \rangle$.

Remark. There is a cyclic subgroup $\langle \tau \rangle \subset S$ of the translations, which is the elementary lattice.

To show that *these are all symmetries*, note that every symmetry of the sine curve preserves the x-axis and is thus either a horizontal translation, a reflection on a vertical line, or a rotation by 180° about a point on the x-axis. Due to the discretely periodic nature of the sin-curve, all possible symmetries are thus the listed ones. □

Exercise 1.1.5. 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.

Solution. Denote $\langle a \rangle$ the cyclic group generated by a. Due to associativity this group is abelian, i.e. $a^n a^m = a^{n+m} = a^m a^n$ as can be checked by making the distinction $n \geq 0$, or $n < 0$. Once this is proven, it is also clear that $(a^m)^n = a^{mn}$, again by the 2 cases for n. □

Exercise 1.1.6. a. Show that a finite group with an even number of elements contains an even number of elements x such that $x^{-1} = x$.

b. State and prove a similar statement for finite groups with an odd number of elements.

Solution. Let $\Omega_2 := \{x \in G : x^2 = \mathrm{id}\}$ and $C := G \setminus \Omega_2$. For $x \in C$ we have $x^-1 \neq x$ and thus $x^{-1} \in C$, i.e. the elements of C come in pairs. If G is finite, then C is also finite and has thus an even number of elements. This leads to:

a. If $(G : 1)$ is even, then $|\Omega_2|$ is also even.

b. If $(G : 1)$ is odd, then also $|\Omega_2|$ is odd.

□

1.2 Subgroups and homomorphisms

Exercise 1.2.1. 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.

Solution. Let $S_\cap$ be the mentioned intersection.

a. Since for all $\alpha \in A$, $\mathrm{id}_G \in S_\alpha$, we also have $\mathrm{id}_G \in S_\cap$. Moreover if $g \in S_\cap$, then $g \in S_\alpha$ for all $\alpha \in A$. But then also $g^{-1} \in S_\alpha$ for the same α and thus $g^{-1} \in S_\cap$. Due to the same argument $g, h \in S_\cap$ implies $g, h \in S_\alpha$ for all $\alpha \in A$. But then $gh \in S_\alpha$ and thus $gh \in S_\cap$. This proves that $S_\cap$ is a subgroup.

b. Let now $S_\alpha \triangleleft G$ be normal subgroups. Then for every $g \in G$ we have $ghg^{-1} \in S_\alpha$. But then also $ghg^{-1} \in S_\cap$. In total $gS_\cap g^{-1} \subset S_\cap$. Since this is true for all $g \in G$, $S_\cap \triangleleft G$ as required.

□

Exercise 1.2.2. 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.

Solution. Let $\sigma \in D_n$ be a reflection, i.e. $\sigma^2 = \mathrm{id}$. Then $\sigma H = \{\sigma, \sigma\tau\}$ while $H\sigma = \{\sigma, \sigma\tau^{-1}\}$. For $n \geq 3$ we know that $\tau^{-1} = \tau^{n-1} \neq \tau$ and therefore these two sets do not coincide. □

Exercise 1.2.3.

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 $S_2 \subset S_1$.

Solution.

a. Let $G = C_2 \times C_2 := \{(a, b) : a, b \in C_2 \cong \mathbb{Z}/(2)\}$ with componentwise operation. Then $C_{0,1} := \mathrm{id} \times C_2$ and $C_{1,0} := C_2 \times \mathrm{id}$ are subgroups, but their union is $G \setminus \{(1, 1)\}$, has only 3 elements and is thus not a subgroup.

b. The cases $S_1 \subset S_2$ and $S_2 \subset S_1$ are clear. Conversely we assume that $S_1 \cup S_2 \subset G$ is a subgroup. If neither subgroup is contained in the other one, then there are $g \in S_1 \setminus S_2$ and $h \in S_2 \setminus S_1$. We know that $y := gh \in S_1 \cup S_2$. W.l.o.g. let $y \in S_1$. But then $h = g^{-1}y \in S_1$ in contradiction to the assumption. Therefore the assumption is wrong and the original claim must be true.

□

Exercise 1.2.4. Show that every group of prime order is simple (i.e. has only trivial subgroups) and cyclic.

Solution. Let G be of prime oder $p \in \mathbb{P}$. Lagrange's theorem shows that every subgroup $S \subset C_p$ has order $d|p$. But the only positive divisors of p are 1 and p. $(S : 1) = 1$ implies $S = \{\mathrm{id}\}$ the trivial subgroup and $(S : 1) = p$ implies $S = G$ the other trivial subgroup.

Consider now the order of the elements $g \in G$. Since $\operatorname{ord} g = (\langle g \rangle : 1)|(G : 1)$ these are also either 1 or p. For $\operatorname{ord} g = 1$ we conclude $g = \mathrm{id}$ and in the other case that $G = \langle g \rangle$ and in particular cyclic. This completes the proof. □

Exercise* 1.2.5. 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.

Solution. The subgroup inclusion pattern is a *partial order*, i.e. any two $S, T \subset G$ can be related as $S \subset T$ or $T \subset S$ or not related at all, and if they are the first two, then $S = T$. Note also that all inclusion chains $S_0 \subset S_1 \subset \dots$ have G as the upper bound. By a proposition in class the supremum $S_\infty := \bigcup_{n\geq 0} S_n$ is a subgroup of G as well.

Therefore given any subgroup H, then we can write down the whole inclusion pattern from H to G. Going along any maximal branch $H = S_0 \subset S_1 \subset S_2 \subset \cdots \subset G$ and omitting G, we see that S_∞ as defined above is a maximal subgroup (because the branch was maximal). Also $H = S_0 \subset S_\infty$ is contained in it. This completes the proof.

Note that the existence of maximal branches requires that either the group is finite or Zorn's lemma (or the axiom of choice). □

Exercise 1.2.6. 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 $H \cap K$.

Solution. Let L_H be a left-coset of H, L_K be a left-coset of K, $L := L_H \cap L_K$ their intersection, and $S := H \cap K$ the intersection of the two subgroups. Assume further that $g \in L$, i.e. the intersection is not empty. Obviously $g \in L_H$ implies $L_H = gH$ and conversely $L_K = gK$. But then $gS \subset L$. On the other hand for $g' \in L$ there is an $h \in H$ and a $k \in K$ such that $gh = g' = gk$. Since G is a group (multiplication with g^{-1} from the left yields) $h = k \in H \cap K = S$. This completes the proof. □

Exercise 1.2.7. 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.

Solution. Denote $\phi^{-1} \colon H \to G : \phi(g) \mapsto g$ the inverse map. Since ϕ is a bijection, this is well defined. Also since ϕ is a homomorphism, we know that $\phi(g_1)\phi(g_2) = \phi(g_1 g_2)$, i.e. $\phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$ for $\phi(g_i) = h_i$. But this is the homomorphism property. □

Exercise 1.2.8. 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.

Solution. Note that the map $\phi^{-1}\colon 2^H \to 2^G$ also maps cosets to cosets, i.e. for $N' := \phi^{-1}(N) \subset G$, then $\phi^{-1}(hN) = gN'$ if there is a $g \in G$ with $\phi(g) = h$ (i.e. $h \in \operatorname{im}\phi$) and $\phi^{-1}(Nh) = N'g$.

a. It follows that $gN' = \phi^{-1}(hN) = \phi^{-1}(Nh) = N'g$ for $h = \phi(g)$, i.e. the left-cosets coincide with the right-cosets.

b. Let conversely ϕ be surjective, $N \triangleleft G$ be a normal subgroup and $N'' := \phi(N)$. We have shown in the lecture that $N'' \subset H$ is a subgroup. Then $hN'' = \phi(gN) = \phi(Ng) = N''h$ for any $g \in G$ with $\phi(g) = h$. But since ϕ is surjective, there is always such a g.

c. We thus need a map that is not surjective and moreover $N_H(\phi(N)) \neq H$, i.e. in particular $\phi(N), H \setminus \phi(N) \not\subset \operatorname{cent} H$. This said, we try, e.g. $G = D_2$, $S = \langle\sigma\rangle \triangleleft G$ the subgroup generated by a rotation, and $H = D_4$. ($S \triangleleft D_2$, because $D_2 \cong C_2 \times C_3$ is abelian.) Then $\phi\colon D_2 \to D_4 : \sigma \mapsto \sigma, \tau_2 \mapsto \tau_4^2$ maps $\phi(N) = \langle\sigma\rangle$. Now $N_H(\langle\sigma\rangle) = \langle\sigma, \tau_4^2\rangle \subsetneq H$ and therefore S is not normal in H. This is actually the example that follows from the next exercise.

□

Exercise 1.2.9. Show that D_4 contains subgroups $A \subset N \subset D_4$ such that $A \triangleleft N$ and $N \triangleleft D_4$, but not $A \triangleleft D_4$.

Solution. Let $N := \langle\sigma, \tau^2\rangle \subset D_4$ the subgroup generated by a reflection and the rotations by 180°. This is normal $N \triangleleft D_4$. Further $A := \langle\sigma\rangle \subset N \subset D_4$. Since N is abelian $A \triangleleft N$. But on the other hand $N_{D_4}(A) = \langle\sigma, \tau^2\rangle \subsetneq D_4$, i.e. not normal in D_4. □

Exercise 1.2.10. Prove that every subgroup of index 2 is normal.

Solution. Let $H \subset G$ be a subgroup of index 2, i.e. $(G : H) = 2$. In particular $G/H = \{H, G \setminus G\}$. But also $H\backslash G = \{H, G \setminus H\}$, i.e. the two cosets are left-cosets as well as right-cosets. Moreover $gH = H$ iff $g \in H$ as well as $Hg = H$ in the same case. Therefore $gH = Hg$ for all $g \in G$. □

Exercise 1.2.11. Prove that the union of an increasing sequence of normal subgroups $N_1 \subset N_2 \subset N_3 \subset \ldots,\ N_i \triangleleft G$ of a group G is normal.

Solution. Let $N_\infty := \bigcup_{n\geq 1} N_n \subset G$ be their union. As shown in class $N_\infty \subset G$ is a subgroup. Let now $g \in G$ and $n \in N_\infty$. But then there is an $m \geq 1$ such that $n \in N_m \triangleleft G$. Therefore $gng^{-1} \in N_m \subset N_\infty$ and so $gN_\infty g^{-1} \subset N_\infty$. But this proves that $N_\infty \triangleleft G$ is normal. □

Exercise 1.2.12.

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.

Solution.

a. Obviously $\phi|X = \psi|X$ is necessary. Since $G = \langle X \rangle$ we know that we can write every element $g \in G$ as a (finite) product of elements in $X \cap \bar{X}$. But since $\phi(x) = \psi(x)$ for all $x \in X \cup \bar{X}$ this implies $\phi(g) = \psi(g)$. Therefore $\phi = \psi$.

b. $V_4 \cong C_2 \times C_2$ abelian, i.e. $V_4 = \langle (12)(34), (13)(24) \rangle$ and each generator has degree 2. But then we can map each of them to any element in V_4, i.e. $\mathrm{End}(V_4) \approx V_4 \times V_4$. The monoid structure is $\mathrm{End}(V_4) \cong \mathrm{End}(\mathbb{F}_2^2)$, i.e. matrix multiplication of linear maps of the (2 dimensional) vector space $\mathbb{F}_2^2$ over $\mathbb{F}_2$ the field with 2 elements.

c. The automorphisms are now these endomorphisms that are invertible, i.e. we cannot map any generator to $\mathrm{id} \in V_4$. But also $\phi((13)(24)) \in \langle \phi((12)(34)) \rangle$ would not permit us to invert the map. In the above isomorphism these are the elements $\mathrm{GL}_2(\mathbb{F}_2)$, i.e. the invertible 2×2 matrices with entries in $\mathbb{F}_2$. In particular these are $\mathrm{Aut}(V_4) \cong \mathrm{GL}_2(\mathbb{F}_2) = \{\mathbb{1}, \binom{1\,0}{1\,1}, \binom{1\,1}{0\,1}, \binom{1\,1}{1\,0}, \binom{0\,1}{1\,0}, \binom{0\,1}{1\,1}\}$ a group with 6 elements. Since the group is not abelian, it must be isomorphic to D_3, namely for $\binom{0\,1}{1\,0} \mapsto \sigma$ (order 2) and $\binom{1\,1}{1\,0} \mapsto \tau$ (order 3), we see that $\mathrm{Aut}(V_4) \cong D_3$.

d. Analogously $D_3 = \langle \sigma, \tau : \sigma^2 = \mathrm{id} = \tau^3, \ldots \rangle$, i.e. it is also generated by 2 elements. Therefore any endomorphism needs to map σ to an element

of degree 2 (or 1). These elements are $O_2 = \{\mathrm{id}, \sigma, \sigma\tau, \sigma\tau^2\}$. Conversely τ needs to be mapped to an element of degree 3 (or 1), which are $N = \{\mathrm{id}, \tau, \tau^2\}$. But we also have to check that the images fulfill the additional relations ..., i.e. $\phi(\sigma\tau\sigma) = \phi(\sigma)\phi(\tau)\phi(\sigma)$. By inspection this is true for all choices $O_2 \times N$ except for $(\mathrm{id}, \tau^{\pm 1})$. Therefore the endomorphisms are $\mathrm{End}(D_3) \approx \{\mathrm{Id}, (\mathrm{id}, \mathrm{id}), (\sigma, \mathrm{id}), (\sigma, \tau^2), (\sigma\tau, \mathrm{id}), (\sigma\tau, \tau), (\sigma\tau, \tau^2), (\sigma\tau^2, \mathrm{id}), (\sigma\tau^2, \tau)$
The multiplication law is

Id	(σ, id)	(σ, τ^2)	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau)$	$(\sigma\tau, \tau^2)$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \tau)$	$(\sigma\tau^2, \tau^2)$
(id, id)	$(\mathrm{id}, \mathrm{id})$	$(\mathrm{id}, \mathrm{id})$	...					
(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)
(σ, τ^2)	(σ, id)	Id	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \tau^2)$	$(\sigma\tau^2, \tau)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau^2)$	$(\sigma\tau, \tau)$
$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \mathrm{id})$	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)	(σ, id)
$(\sigma\tau, \tau)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau^2)$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \tau)$	$(\sigma\tau^2, \tau^2)$	(σ, id)	Id	(σ, τ^2)
$(\sigma\tau, \tau^2)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau)$	(σ, id)	(σ, τ^2)	Id	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \tau^2)$	$(\sigma\tau^2, \tau)$
$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$	$(\sigma\tau^2, \mathrm{id})$
$(\sigma\tau^2, \tau)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau^2)$	(σ, id)	Id	(σ, τ^2)	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau)$	$(\sigma\tau, \tau^2)$
$(\sigma\tau^2, \tau^2)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau)$	$(\sigma\tau, \mathrm{id})$	$(\sigma\tau, \tau^2)$	$(\sigma\tau, \tau)$	(σ, id)	(σ, τ^2)	Id

The invertible elements are $\mathrm{Aut}(D_3) = \{\mathrm{Id}, (\sigma, \tau^2), (\sigma\tau, \tau^2), (\sigma\tau^2, \tau), (\sigma\tau^2, \tau^2)\}$ a group with 4 elements which is not cyclic, thus $\mathrm{Aut}(D_3) \cong C_2 \times C_2$.

□