# Aluffi, *Algebra: Chapter 0*

Danny Nygård Hansen

17th January 2022

## I • Preliminaries: Set theory and categories

## II • Groups, first encounter

### *1. Definition of group*

EXERCISE 1.4

Suppose that $g^2 = e$ for all elements $g$ of a group $G$; prove that $G$ is commutative.

SOLUTION. The hypothesis implies that $g = g^{-1}$ for all $g \in G$. For $g, h \in G$ we thus have

$$gh = (gh)^{-1} = h^{-1}g^{-1} = hg$$

as desired. □

EXERCISE 1.8

Let $G$ be a finite abelian group with exactly one element $f$ of order 2. Prove that $\prod_{g \in G} g = f$.

SOLUTION. Every element $g$ in $G$ different from $e$ and $f$ has order greater than two, hence $g \neq g^{-1}$. The product $\prod_{g \in G \setminus \{e,f\}} g$ therefore contains all such elements along with their inverses, and thus equals $e$. The claim follows. □

EXERCISE 1.9

Let $G$ be a finite group, of order $n$, and let $m$ be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if $n$ is even, then $G$ necessarily contains elements of order 2.

SOLUTION. Let $G'$ denote the set of elements in $G$ with order greater than 2. We claim that $|G'|$ is even, and we give two arguments for this fact. First, simply notice that the elements of $G'$ come in pairs $\{g, g^{-1}\}$ with $g \neq g^{-1}$.

For a more precise argument (using group theory language we haven't seen yet), consider the inversion map $g \mapsto g^{-1}$. This restricts to a well-defined map $\iota \colon G' \to G'$, and $\iota$ is a permutation of $G'$. Letting the cyclic group $\langle \iota \rangle \leq S_{G'}$ act on $G'$ splits $G'$ into orbits of size two, and since these orbits determine a partition of $G'$, $|G'|$ must be even.

Now notice that $G'$ contains $n - m - 1$ elements since $e$ has order 1, hence $n - m$ is odd. If $n$ is even, then $m$ must be odd and thus at least 1. $\square$

EXERCISE 1.11

Prove that for all $g, h$ in a group $G$, $|gh| = |hg|$.

SOLUTION. Let $a, g \in G$, and let $n = |g|$. Then

$$(aga^{-1})^n = ag^n a^{-1} = e,$$

so the order of $aga^{-1}$ divides the order of $g$. Substituting $g \to aga^{-1}$ and $a \to a^{-1}$ shows that $|g|$ also divides $|aga^{-1}|$, so $|g| = |aga^{-1}|$. Finally substituting $g \to gh$ and $a \to h$ proves the claim.

Alternatively, the conjugation map $g \mapsto aga^{-1}$ is an isomorphism, so it preserves orders. $\square$

EXERCISE 1.13

Give an example showing that $|gh|$ is not necessarily equal to $\operatorname{lcm}(|g|, |h|)$, even if $g$ and $h$ commute.

SOLUTION. In $\mathbb{Z}/4\mathbb{Z}$ we have $|[2]_4| = 2$ and $|[2]_4 + [2]_4| = |[0]_4| = 1$. $\square$

EXERCISE 1.14

Prove that if $g$ and $h$ commute *and* $\gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$.

SOLUTION. First recall that $\operatorname{lcm}(|g|, |h|) = |g||h|$, so Proposition 1.14 implies that $|gh|$ divides $|g||h|$. Conversely, letting $N = |gh|$ we have

$$e = (gh)^{|g|N} = g^{|g|N} h^{|g|N} = h^{|g|N},$$

so $|h|$ divides $|g|N$. But since $|g|$ and $|h|$ are relatively prime, $|h|$ divides $N$. So does $|g|$, so again using relative primality we find that $|g||h|$ divides $N$. In total, $|gh| = |g||h|$. $\square$

## *2. Examples of groups*

EXERCISE 2.1

One can associate an $n \times n$ matrix $M_\sigma$ with a permutation $\sigma \in S_n$ by letting the entry at[1] $(i, \sigma(i))$ be 1 and letting all other entries be 0. Prove that, with this notation,

$$M_\sigma M_\tau = M_{\tau\sigma}$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices.

SOLUTION. Notice that, for $1 \leq i, j \leq n$,

$$(M_\sigma M_\tau)_{ij} = \sum_{k=1}^{n} (M_\sigma)_{ik}(M_\tau)_{kj},$$

and that the summand $(M_\sigma)_{ik}(M_\tau)_{kj}$ is 1 just when $\sigma(i) = k$ and $\tau\sigma(i) = j$, and 0 otherwise. Thus,

$$(M_\sigma M_\tau)_{ij} = \begin{cases} 1, & \tau\sigma(i) = j, \\ 0, & \text{otherwise}, \end{cases}$$

which is just the definition of the matrix $M_{\tau\sigma}$. $\square$

EXERCISE 2.13

Prove that if $\gcd(m, n) = 1$, then there exist integers $a$ and $b$ such that

$$am + bn = 1.$$

Conversely, prove that if $am+bn = 1$ for some integers $a$ and $b$, then $\gcd(m, n) = 1$.

SOLUTION. By Corollary 2.5, the class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. Hence there exists an $a \in \mathbb{Z}$ such that $a[m]_n = [1]_n$. But then $qn = am - 1$ for some $q \in \mathbb{Z}$, i.e. $am + (-q)n = 1$.

Conversely, if $am + bn = 1$ and $d$ divides both $m$ and $n$, then $d$ also divides 1 and hence $d = \pm 1$. $\square$

## *3. The category* **Grp**

[1] Contrary to Aluffi, we prefer to let permutation act on the left.

**Exercise 3.3**

Show that if $G, H$ are *abelian* groups, then $G \times H$ satisfies the universal property for coproducts in **Ab**.

**Solution.** Let $\varphi_G \colon G \to K$ and $\varphi_H \colon H \to K$ be homomorphisms into an abelian group $K$. Define a map $\psi \colon H \times G \to K$ by

$$\psi(g,h) = \varphi_G(g)\varphi_H(h).$$

We first show that $\psi$ is a group homomorphism. For $g_1, g_2 \in G$ and $h_1, h_2 \in H$ we have

$$\begin{aligned}
\psi((g_1,h_1)(g_2,h_2)) = \psi(g_1g_2, h_1h_2) &= \varphi_G(g_1g_2)\varphi_H(h_1h_2) \\
&= \varphi_G(g_1)\varphi_G(g_2)\varphi_H(h_1)\varphi_H(h_2) \\
&= \varphi_G(g_1)\varphi_H(h_1)\varphi_G(g_2)\varphi_H(h_2) \\
&= \psi(g_1,h_1)\psi(g_2,h_2).
\end{aligned}$$

In the third equality we used that $K$ is abelian. Next we show that the diagram

$$\begin{tikzcd}
G \arrow[dr, "\iota_G"] \arrow[drr, bend left, "\varphi_G"] & & \\
& G \times H \arrow[r, "\psi"] & K \\
H \arrow[ur, "\iota_H"'] \arrow[urr, bend right, "\varphi_H"'] & &
\end{tikzcd}$$

commutes, where $\iota_G(g) = (g, e_H)$ and $\iota_H(h) = (e_G, h)$. For the upper triangle we have

$$(\psi \circ \iota_G)(g) = \psi(g, e_G) = \varphi_G(g)\varphi_H(e_G) = \varphi_G(g)e_K = \varphi_G(g),$$

and similarly for the lower triangle. □

**Exercise 3.4**

Let $G, H$ be groups, and assume that $G \cong H \times G$. Can you conclude that $H$ is trivial?

**Solution.** Let $H$ be any nontrivial group, and let $G = \prod_{n\in\mathbb{N}} H$. Then the map $\varphi \colon G \to H \times G$ given by

$$\varphi(h_1, h_2, h_3, \dots) = \big(h_1, (h_2, h_3, \dots)\big)$$

is an isomorphism. □

EXERCISE 3.5

Prove that $\mathbb{Q}$ is not the direct product of two nontrivial groups.

SOLUTION. Let $G$ and $H$ be groups such that there is an isomorphism $\varphi\colon \mathbb{Q} \to G \times H$. Assume without loss of generality that $G$ is nontrivial, and consider the map $\varphi_G = \pi_G \circ \varphi$. We claim that $\varphi_G$ is injective.

First notice that if $g \in G$ has finite order then $g = 0_G$, since $(g, 0_H)$ has finite order in $G \times H$. Let $p, q \in \mathbb{Z}$ with $p, q \neq 0$, and notice that $\varphi_G(p/q) = 0_G$ implies that

$$0_G = q\varphi_G\left(\frac{p}{q}\right) = \varphi_G(p) = p\varphi_G(1).$$

Hence $\varphi_G(1) = 0_G$, and so $\mathbb{Z} \subseteq \ker \varphi_G$. Furthermore, if $a, b \in \mathbb{Z}$ with $b \neq 0$, then

$$b\varphi_G\left(\frac{a}{b}\right) = \varphi_G(a) = 0_G,$$

so $\varphi_G(a/b)$ has finite order and hence equals $0_G$. Thus if $\ker \varphi_G$ is nontrivial, then $\ker \varphi_G = \mathbb{Q}$. But since $\varphi_G$ is surjective and $G$ is nontrivial, this is impossible. Hence $\varphi_G$ is injective. On the other hand, the kernel of $\varphi_G$ is clearly $1 \times H$, so $H$ must be trivial. $\square$

EXERCISE 3.6

Consider the product $C_2 \times C_3$ of the cyclic groups $C_2, C_3$. By Exercise 3.3, this group is a coproduct of $C_2$ and $C_3$ in **Ab**. Show that it is *not* a coproduct of $C_2$ and $C_3$ in **Grp**.

SOLUTION. Denote by $g$ and $h$ generators of $C_2$ and $C_3$ respectively, and define group homomorphisms $\varphi_2\colon C_2 \to S_3$ and $\varphi_3\colon C_3 \to S_3$ by

$$\varphi_2(g) = (1\ 2) \quad \text{and} \quad \varphi_3(h) = (1\ 2\ 3).$$

Assume that $C_2 \times C_3$ is a coproduct of $C_2$ and $C_3$ in **Grp**. Then there exists a homomorphism $\psi\colon C_2 \times C_3 \to S_3$ such that $\varphi_2 = \psi \circ \iota_2$ and $\varphi_3 = \psi \circ \iota_3$. Since $C_2 \times C_3$ is commutative, it follows that

$$(1\ 2)(1\ 2\ 3) = \psi(\iota_2(g)\iota_3(h)) = \psi(\iota_3(h)\iota_2(g)) = (1\ 2\ 3)(1\ 2).$$

But this is false, so $C_2 \times C_3$ is not a coprodut of $C_2$ and $C_3$ in **Grp**. $\square$

EXERCISE 3.8

Define a group $G$ with two generators $x, y$ subject (only) to the relations $x^2 = e_G$, $y^3 = e_G$. Prove that $G$ is a coproduct of $C_2$ and $C_3$ in **Grp**.

SOLUTION. Denote the generators of $C_2$ and $C_3$ by $g$ and $h$ respectively, and let $\varphi_2\colon C_2 \to H$ and $\varphi_3\colon C_3 \to H$ be homomorphisms into a group $H$. Define a map $\psi\colon G \to H$ by letting $\psi(x) = \varphi_2(g)$ and $\psi(y) = \varphi_3(h)$ and extending to all elements in $G$ by requiring that $\psi$ be a homomorphism. Then $\varphi_2 = \psi \circ \iota_2$ and $\varphi_3 = \psi \circ \iota_3$, so $G$ is indeed a coproduct. $\square$

## 4. *Group homomorphisms*

EXERCISE 4.1

Check that the function $\pi_m^n$ defined in §4.1 is well-defined and makes the diagram commute. Verify that it is a group homomorphism.

SOLUTION. Recall that $\pi_m^n\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is defined by $\pi_m^n([a]_n) = [a]_m$, assuming that $m \mid n$. To show that this is well-defined, let $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{n}$. This means that $n \mid a - b$, and hence that $m \mid a - b$, i.e. that $a \equiv b \pmod{m}$. In other words, $[a]_n = [b]_n$ implies that $[a]_m = [b]_m$, and thus $\pi_m^n$ is well-defined. It is also obvious that the diagram

$$\begin{tikzcd} \mathbb{Z} \arrow[d, "\pi_n"'] \arrow[dr, "\pi_m"] & \\ \mathbb{Z}/n\mathbb{Z} \arrow[r, "\pi_m^n"'] & \mathbb{Z}/m\mathbb{Z} \end{tikzcd}$$

commutes, since $\pi_n(a) = [a]_n$ and $\pi_m(a) = [a]_m$.

Finally we show that $\pi_m^n$ is a homomorphism. For $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} \pi_m^n([a]_n + [b]_n) &= \pi_m^n([a+b]_n) = [a+b]_m = [a]_m + [b]_m \\ &= \pi_m^n([a]_n) + \pi_m^n([b]_n) \end{aligned}$$

as desired. $\square$

EXERCISE 4.8

Let $G$ be a group, and let $g \in G$. Prove that the function $\gamma_g\colon G \to G$ defined by $\gamma_g(a) = gag^{-1}$ is an automorphism of $G$. (The automorphisms $\gamma_g$ are called 'inner' automorphisms of $G$.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if $G$ is abelian.

SOLUTION. For $a, b \in G$ we have

$$\gamma_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \gamma_g(a)\gamma_g(b),$$

so $\gamma_g$ is a homomorphism. It is obviously invertible with $\gamma_g^{-1} = \gamma_{g^{-1}}$, hence an isomorphism.

Now let also $h \in G$. Then

$$(\gamma_{gh})(a) = (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = \gamma_g(hah^{-1}) = (\gamma_g \circ \gamma_h)(a),$$

so $g \mapsto \gamma_g$ is a homomorphism. □

**EXERCISE 4.9**

Prove that if $m, n$ are positive integers such that $\gcd(m,n) = 1$, then $C_{mn} \cong C_m \times C_n$.

SOLUTION. The map $\pi = (\pi_m^{mn}, \pi_n^{mn})$ is a group homomorphism, and since the sets $C_{mn}$ and $C_m \times C_n$ have the same cardinality, it suffices to show that $\pi$ is injective. Using additive notation, if $\pi([a]_{mn}) = \pi([b]_{mn})$ then $[a]_m = [b]_m$, i.e. $m \mid a-b$. Similarly $n \mid a-b$, and since $\gcd(m,n) = 1$ we have $mn \mid a-b$. It follows that $[a]_{mn} = [b]_{mn}$ as desired. □

## 5. *Free groups*

## 6. *Subgroups*

**EXERCISE 6.6**

Prove that the union of a family of subgroups of a group $G$ is not necessarily a subgroup of $G$. In fact:

(a) Let $H, H'$ be subgroups of a group $G$. Prove that $H \cup H'$ is a subgroup of $G$ only if $H \subseteq H'$ or $H' \subseteq H$.

(b) On the other hand, let $H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots$ be subgroups of a group $G$. Prove that $\bigcup_{i \geq 0} H_i$ *is* a subgroup of $G$.

SOLUTION. (a) Assume that $H \cup H'$ is a subgroup of $G$ and let $h \in H$ and $h' \in H'$. Then $hh' \in H \cup H'$, say $hh' \in H$. But then $h' = h^{-1}(hh') \in H$, so $h' \in H$ and hence $H' \subseteq H$. Similarly if $hh' \in H'$.

(b) Write $H = \bigcup_{i \geq 0} H_i$. If $g, h \in H$, then $g \in H_i$ and $h \in H_j$ for some $i, j \in \mathbb{N}$.[2] Hence $g, h \in H_i \cup H_j = H_{i \vee j} \subseteq H$. We furthermore have $g^{-1} \in H_i \subseteq H$. □

[2] The natural numbers include zero.

**Exercise 6.7**

Show that *inner* automorphisms (cf. Exercise 4.8) form a subgroup of $\mathrm{Aut}(G)$; this subgroup is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G)$ is trivial if and only if $G$ is abelian. Deduce that if $\mathrm{Aut}(G)$ is cyclic, then $G$ is abelian.

Solution. It is clear that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Assume that $\mathrm{Inn}(G)$ is cyclic, and let $a \in G$ be such that $\gamma_a$ generates $\mathrm{Inn}(G)$. For $g \in G$ we then have $\gamma_g = \gamma_a^n = \gamma_{a^n}$ for some $n \in \mathbb{Z}$. Hence

$$gag^{-1} = \gamma_g(a) = \gamma_{a^n}(a) = a^n a a^{-n} = a,$$

so $a$ commutes with every $g \in G$. For $b \in G$ we thus have

$$\gamma_g(b) = \gamma_{a^n}(b) = a^n b a^{-n} = b,$$

so $\gamma_g$ is the identity map for every $g \in G$. Therefore $\mathrm{Inn}(G)$ is trivial, which is obviously equivalent to $G$ being abelian.

Finally, if $\mathrm{Aut}(G)$ is cyclic then Propositions 6.9 and 6.11 imply that $\mathrm{Inn}(G)$ is also cyclic. But then $G$ is abelian. $\square$