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. $\square$

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. $\square$

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 ι 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. □

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. □

2. *Examples of groups*

EXERCISE 2.1

One can associate an $n \times n$ matrix M_σ 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 $1 \leq i, j \leq n$,

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

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

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**

4. *Group homomorphisms*

Exercise 4.1

Check that the function π_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 π_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 π^n_m is a homomorphism. For $a,b \in \mathbb{Z}$ we have

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

as desired. □

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 $\pi = (\pi^{mn}_m, \pi^{mn}_n)$ 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 π 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.