1 Definition of groups

Definition 1.0.1. A group is a groupoid with a single object. (Groupoids are categories in which every morphism is an isomorphism).

1.1 Exercises

1. (1.1) Consider a group G, we show that G is the group of isomorphisms of a groupoid. Such groupoid C will have a single obejct G. Morphisms in C will be $f_g : G \to gG$, which is a bijection. Hence, $\mathrm{Aut}_{\mathsf{C}}(G)$ forms a group.

2. (1.4) For $g, h \in G$, we have $(gh)^{-1} = h^{-1}g^{-1} = hg$ since $h^2 = g^2 = e$. Therefore, $gh = hg$ or G is commutative.

3. (1.8) Here G should be an finite abelian group, otherwise the problem is false. If G is abelian then for $g \in G, g \neq f$ we know $g^{-1} \neq g$ so we can group g with g^{-1} in the product $\prod_{g \in G} g$. What lefts is f, as desired.

4. (1.9) If $f^2 = e$ then f is equal to its own inverse. Therefore, excluding m elements in G that whose inverse is itself and excluding the identity e, we left with pairs (g, g^{-1}). Therefore, number of such pairs is $\frac{1}{2}(n - m - 1)$. This implies $n - m$ is odd.

5. (1.10) Proposition 1.13 tells us that $|g^2| = \frac{|g|}{\gcd(|g|,2)} = |g|$.

6. (1.11) We first show $|aga^{-1}| = |g|$. Indeed, we have $(aga^{-1})^k = ag^ka^{-1}$. This follows $|aga^{-1}|$ divides $|g|$ and that $|g|$ divides $|aga^{-1}|$. Hence, $|aga^{-1}| = |g|$.

   Back to our problem, we have $|gh| = |g(hg)g^{-1}| = |hg|$ so we are done.

7. (1.12) Yes, verify it.

8. (1.13) We choose group $(\mathbb{Z}/6\mathbb{Z}, +)$ where $g = [2]_6, h = [4]_6$ then $|g| = |h| = 3$ so $\mathrm{lcm}(|g|, |h|) = 3$ and also g and h commutes. However, $|gh| = |[0]_6| = 1$.

9. (1.14) Let $|gh| = N$ then since g and h commutes, we have $(gh)^N = g^Nh^N = e$ so $g^N = (h^{-1})^N$. This follows $|g^N| = |h^{-N}| = |h^N|$. According to proposition 1.13, we have

   $$|g^N| = \frac{|g|}{\gcd(N, |g|)} = \frac{|h|}{\gcd(N, |h|)} = |h^N|.$$

   Since $\gcd(|g|, |h|) = 1$ so this implies $|g| = \gcd(N, |g|)$ so $|g|$ divides N. Similarly, $|h|$ divides N. Therefore, $\mathrm{lcm}(|g|, |h|) = |g| \cdot |h|$ divides N. On the other hand, from proposition 1.14, we know $N = |gh|$ divides $\mathrm{lcm}(|g|, |h|) = |g| \cdot |h|$ so we conclude $|gh| = |g||h|$.

10. (1.15) We want to show that if $g \in G$ is an element of maximal finite order then for any $h \in G$, we have $|h|$ divides $|g|$. Assume the contrary that $|h|$ does not divide $|g|$, there exists a prime p such that $|h| = p^m r$ and $|g| = p^n s$ where $\gcd(r, p) = \gcd(r, s) = 1$ and $m > n$. From proposition 1.13, we have $|h^r| = \frac{|h|}{\gcd(|h|,r)} = p^m$ and similarly $|g^{p^n}| = s$. Therefore, $\gcd(|h^r|, |g^{p^n}|) = 1$ so from Exercise I.1.14, we have $|g^{p^n}h^s| = |g^{p^n}||h^s| = p^m s > |g| = p^n s$ since $m > n$. This causes a contradiction so we must have $|h|$ divides $|g|$.

2 Examples of groups

Definition 2.0.1. Let A be a set. The *symmetry group* of A, denoted S_A, is the group $\mathrm{Aut}_{\mathsf{Set}}(A)$. The group of permutations of the set $\{1, 2, \ldots, n\}$ is denoted by S_n.

2.1 Exercises

1. (2.2) It suffices to show that for any n, S_n contains an element of order n. Indeed, if this is true then for $d \le n$, we can just fix $n - d$ elements and let other d elements form a permutation of order d in S_d. This will create an element of order d in S_n.

   Now, the following element has order n

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ n & 1 & 2 & 3 & \cdots & n-2 & n-1 \end{pmatrix}$$

2. (2.3) See previous exercise II.2.2. Essentially we choose the $1, 2, \ldots, n$ to form an element in S_n of order n and then fix the rest of $\mathbb{N}$.

3. (2.5) The three relations are $x^2 = y^n = e$ and $yx = xy^{n-1}$.

4. (2.6) Choose $g = x, h = xy$ then $|g| = 2$ and $h^2 = (xy)^2 = xyxy = x(xy^{-1})y = e$ so $|h| = 2$. However, $|gh| = |y| = n$.

5. (2.7) We want to find an element in D_{2n} for $n \ge 3$ that commutes with other element. We will use notation for D_{2n} given in Exercise II.2.5, i.e. $D_{2n} = \{e, y, \ldots, y^{n-1}, x, xy, \ldots, xy^{n-1}\}$.

   Such element cannot be x since $xy \ne yx$.

   If such element is y^i for some $1 \le i \le n-1$ then we need $y^i x = xy^i$. On the other hand, we have $yx = xy^{-1}$ from Exer II.2.5 or $y = xy^{-1}x$ so $y^i x = (xy^{-1}x)^i x = xy^{-i}$. This means $xy^{-i} = xy^i (= y^i x)$ or $y^{2i} = e$. This happens when $2 \mid n$. We should check that $y^{n/2}$ commutes with other elements of D_{2n}, i.e. elements of the form xy^i, which is true.

   Such element cannot be xy^i where $1 \le i \le n-1$ since we need $(xy^i)y = y(xy^i)$ but $y(xy^i) = (yx)y^i = (xy^{-1})y^i = xy^{i-1}$ while $(xy^i)y = xy^{i+1}$. Since $n \ge 3$ and $|y| = n$ so $xy^{i-1} \ne xy^{i+1}$.

   Thus, for n odd, our answer is $\{e\}$. For n even, our answer is $\{e, y^{n/2}\}$.

6. (2.8)

3 The category Grp

3.1 Group homomorphisms

Remark 3.1.1. Note how the author motivates the definition of group homomorphims. One needs to define a group homomorphism $\varphi : (G, m_G) \to (H, m_H)$ that somehow connects operations m_G on G with m_H on H. This suggests to find a function $(\varphi \times \varphi) : G \times G \to H \times H$ such that the diagram commutes.

$$\begin{tikzcd} G \times G \arrow[r, "\varphi\times\varphi"] \arrow[d, "m_G"'] & H \times H \arrow[d, "m_H"] \\ G \arrow[r, "\varphi"'] & H \end{tikzcd}$$

The choice of $\varphi \times \varphi$ is explained naturally from the universal property of products, as in Exercise II.3.1.

3.2 Exercises

1. (3.1) Consider the category $\mathsf{C}_{H,H}$ where $H \times H$ is the final object with two morphisms $\pi_H, \pi'_H : H \times H \to H$ where π_H sends $(h_1, h_2) \mapsto h_1$ while π'_H sends $(h_1, h_2) \mapsto h_2$. Consider object $G \times G$ in C with two morphisms $\pi_G, \pi'_G : G \times G \to H$ where the first one sends $(g_1, g_2) \mapsto g_1 \mapsto \varphi(g_1)$ while the second one sends $(g_1, g_2) \mapsto g_2 \mapsto \varphi(g_2)$. According to the universal property of products, there exists a unique morphism $(\varphi \times \varphi) : G \times G \to H \times H$ such that the following diagram commutes

$$\begin{tikzcd} & & H \\ G \times H \arrow[r, "\varphi\times\varphi"] \arrow[urr, bend left, "\pi_G"] \arrow[drr, bend right, "\pi'_G"'] & H \times H \arrow[ur, "\pi_H"] \arrow[dr, "\pi'_H"'] & \\ & & H \end{tikzcd}$$

This implies $\varphi(g_1, g_2) = (\varphi(g_1), \varphi(g_2))$ for all $g_1, g_2 \in G$, as desired.

2. (3.2) Because $(\psi \times \psi)(\varphi \times \varphi)$ makes the large rectangle in the diagram in §II.3.2 commutes and from previous exercise I.3.1, we know there exists exactly one such morphism $(\psi\varphi) \times (\psi\varphi)$ so $(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi)$.

3. (3.3) Not hard.

4. (3.4) No. Choose $G = \mathbb{Z}[x]$ to be a group under addition, $H = \mathbb{Z}$ then $G \times Z \cong G$. Indeed, consider the group isomorphism sending $(f(x), n) \mapsto x \cdot f(x) + n$.

5. (3.5) If $\mathbb{Q} \cong G \times H$ where G, H are nontrivial group. Let g, h be nontrivial elements in G, H, respectively. Suppose the isomorphism $\varphi : G \times H \to \mathbb{Q}$ send (g, h) and (g, e_H) to two nonzero rational numbers x, y. Since $x, y \in \mathbb{Q}$ and $xy \neq 0$, there exists integers m, n such that $mx = ny$. This follows $m\varphi(g, h) = n\varphi(g, e_H)$ so $(mg, mh) = (ng, e_H)$. Two elements of $G \times H$ are the same iff $mg = ng$ and $mh = e_H$. This implies h has finite order in H. Similarly, g has finite order in G. Thus, (g, h) has finite order in $G \times H$. However, any nonzero element in $(\mathbb{Q}, +)$ does not have finite order. Thus, $\mathbb{Q}$ cannot be the direct product of two nontrivial groups.

6. (3.6) From §II.2.1, we can write group S_3 as $S_3 = \{e, x, y, xy, y^2, xy^2\}$ where $x^2 = e, y^3 = e, yx = xy^2$. We construct injective homomorphisms $f_2 : C_2 \to S_3$ as $[1]_2 \mapsto x, [0]_2 \mapsto e$ and $f_3 : C_3 \to S_3$ as $[0]_3 \mapsto e, [1]_3 \mapsto y, [2]_3 \mapsto y^2$.

   If $C_2 \times C_3$ is a coproduct of C_3 then there exists a group homomorphism $\sigma : C_2 \times C_3 \to S_3$ making following diagram commutes

$$\begin{tikzcd}
C_2 \arrow[dr, "\pi_2"] \arrow[drr, bend left, "f_2"] & & \\
& C_2 \times C_3 \arrow[r, "\sigma"] & S_3 \\
C_3 \arrow[ur, "\pi_3"'] \arrow[urr, bend right, "f_3"'] & &
\end{tikzcd}$$

   where $\pi_2 : C_2 \to C_2 \times C_3$ and $\pi_3 : C_3 \to C_2 \times C_3$ be any group homomorphisms This means $(\sigma\pi_2)([1]_2) = f_2([1]_2) = x$ and $(\sigma\pi_3)([1]_3) = f_3([1]_3) = y$. Since $C_2 \times C_3$ is a commutative group so

$$\begin{aligned}
xy &= \sigma(\pi_2([1]_2))\sigma(\pi_3([1]_3)), \\
&= \sigma\left(\pi_2([1]_2)\pi_3([1]_3)\right), \\
&= \sigma(\pi_3([1]_3))\sigma(\pi_2([1]_2)), \\
&= yx.
\end{aligned}$$

   This is not true so such group homomorphism σ does not exist.

7. (3.8) Define $\pi_2 : C_2 \to G$ as $[0]_2 \mapsto e, [1]_2 \mapsto x$ and $\pi_3 : C_3 \to G$ as $[0]_3 \mapsto e, [1]_3 \mapsto y, [2]_3 \mapsto y^2$. One can check that π_2, π_3 are indeed group homomorphisms. Then we proceed to show $G = C_2 \star C_3$ is indeed coproduct of C_2 and C_3 in Grp.

8. (3.7) Why did Aluffi ask exercise II.3.7 before exercise II.3.8? From exercise II.3.8, we know about $C_2 \star C_3$ which is generated by x_2, y_2 subject to $x_2^2 = y_2^3 = e$. Say $\mathbb{Z} \star \mathbb{Z}$ is generated by x_1, y_2 subject to no relations. Consider functions $\varphi : \mathbb{Z} \star \mathbb{Z} \to C_2 \star C_3$ such that $\varphi(x_1) = x_2, \varphi(y_1) = y_2$ then generate φ from this so that it is a group homomorphism. We can see that φ is also surjective.

9. (3.9) From Exercise I.5.12, we know that fiber products in Set for two morphisms φ, β is $G = \{(a, b) : a \in A, b \in B, \varphi(a) = \beta_b\}$. One can show that this is also a fiber product in Grp from following steps:

(a) Define operation on G so G is an abelian group. One can take a guess to see $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1, b_2)$ satisfies.

(b) Define group homomorphisms π_A, π_B from A, B to G. Obviously $\pi_A(a, b) = a$ and $\pi_B(a, b) = b$ and they are indeed group homomorphisms.

(c) Show D final object in $\mathsf{Ab}_{\alpha,\beta}$. Our unique morphism $\sigma : D \to Z$ given $f_A : A \to Z$ and $f_B : B \to Z$ is $\sigma(g) = (f_A(g), f_B(g))$.

So far, fibered product in Ab is "the same as" fibered product in Set. For fibered coproduct, the situation is a bit harder since from Exercise I.5.12, fibered coproduct in Set is $(C/\sim) \coprod (A \setminus \alpha(C)) \coprod (B \setminus \beta(C))$ which we don't know how to construct a group from this set. TRY THIS again after learning §II.8.

4 Group homomorphisms

4.1 Exercises

1. (4.1) $\pi_m^n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $m \mid n$ defined as $\pi_m^n([a]_n) = [a]_m$. It is well-defined since if $[a]_n = [b]_n$ then $n \mid (a-b)$ then $m \mid n \mid (a-b)$ so $[a]_m = [b]_m$ or $\pi_m^n([a]_n) = \pi_m^n([b]_n)$.

2. (4.2) $\pi_2^4 \times \pi_2^4([2]_4) = \pi_2^4 \times \pi_2^4([0]_4) = ([0]_2, [0]_2)$ so $\pi_2^4 \times \pi_2^4$ not a bijection, so not an isomorphism.

   No isomorphism $C_4 \to C_2 \times C_2$ since every element of $C_2 \times C_2$ has order at most 2 but $[1]_4 \in C_4$ has order 4.

3. (4.3) Use the map $G \to \mathbb{Z}/n\mathbb{Z}$ defined as $g^i \mapsto [i]_n$.

4. (4.4) No isomorphism from $\mathbb{Z}$ to $\mathbb{Q}$ (or $\mathbb{R}$) since any $n \in \mathbb{Z}$ then $n = n \cdot 1$ but this properties does not occur in $\mathbb{Q}$ or $\mathbb{R}$, i.e. not every $x \in \mathbb{Q}$ or $\mathbb{R}$ satisfies $x = n \cdot 1$ for some $n \in \mathbb{Z}$.

   No isomorphism $\mathbb{Q}$ to $\mathbb{R}$ because no surjective function $\mathbb{Q} \to \mathbb{R}$.

5. (4.5) $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ not isomorphic since $i \in C$ has order 4 while $\mathbb{R} \setminus \{0\}$, except for ± 1, no ohter elements has finite order.

6. (4.6) No, $(\mathbb{Q}, +0)$ has elements of finite order of form $1/m$ with $m \neq 0, m \in \mathbb{Z}_{>0}$. But $(\mathbb{Q}^{>0}, \cdot)$, except for ± 1, no other element has finite order.

7. (4.7) Not hard.

8. (4.8) γ_g is a homomorphism with inverse is $\gamma_{g^{-1}}$. The function $\varphi : G \to \text{Aut}\,(G)$ is homomorphism since $\gamma_{g_1 g_2} = \gamma_{g_1}\gamma_{g_2}$.

9. (4.9) Define $\varphi : C_m \times C_n \to C_{mn}$ defined as $\varphi([a]_m, [b]_n) = [c]_{mn}$ such that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$. This c exists since $\gcd(m, n) = 1$ according to Chinese Remainder Theorem.

10. (4.10) From exercise 4.9, we know $(\mathbb{Z}/pq\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ but every $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ has order at most $\text{lcm}\,(p-1, q-1) < (p-1)(q-1)$ so every element in $(\mathbb{Z}/pq\mathbb{Z})^*$ has order less than $(p-1)(q-1)$, which implies it is not cyclic (exercise 4.3).

11. (4.11) Let $g \in G = (\mathbb{Z}/p\mathbb{Z})^*$ be element of maximal order. From exercise 1.15, for all $h \in G$, we must have $|h|$ divides $|g|$ so $h^{|g|} = 1$. From our assumed result, we know there are at most $|g|$ solutions for $h^{|g|} = 1$. As $h^{|g|} = 1$ is true for any $h \in G$ so there are at least $p-1$ solutions for $h^{|g|} = 1$. This follows $|g| \geq p-1$ but also $|g| \leq |G| = p-1$ so $|g| = p-1$ so G has element of order $|G|$, which means $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

12. (4.12) Order of $[9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})^*$ is 15. $x^3 - 9 = 0$ does not have solution in $(\mathbb{Z}/31\mathbb{Z})^*$. This is because $9^{15} \equiv 1 \pmod{31}$ so $(x^3)^{15} \equiv 1 \pmod{31}$ or $x^{45} = 1$. We also know that $x^{30} = 1$ since $(\mathbb{Z}/31\mathbb{Z})^*$ is cyclic. This follows $|x|$ divides $\gcd(30, 45) = 15$. But then $9^5 = x^{15} = 1$ implies $9^5 = 1$, a contradiction. Thus $x^3 - 9 = 0$ does not have solution in $(\mathbb{Z}/31\mathbb{Z})^*$.

13. (4.13) For $\varphi \in \mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ then $\varphi(0,0) = (0,0)$ so φ essentially permutation of $(0,1),(1,1),(1,0)$ of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong S_3$.

14. (4.14) Each $\varphi_a \in G = \mathrm{Aut}_{\mathrm{Grp}}(C_n)$ can be generated by $\varphi_a([1]_n) = [a]_n$, which implies $\varphi_a([m]_n) = m \cdot [a]_n = [ma]_n$. Note that φ is an automorphism iff $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Therefore, consider the function $\pi : G \to (\mathbb{Z}/n\mathbb{Z})^*$ defined as $\pi(\varphi_a) = [a]_n$. One can show this is an automorphism since it is bijective (as shown) and $\varphi_a \circ \varphi_b = \varphi_{ab}$.

15. (4.15)

References

algchap0 [1] Paolo Aluffi. Algebra: Chapter 0