Chapter 2

Groups: First encounter

Problem 1.1. Write a careful proof that every group is the group of isomorphisms of a groupoid. In particular, every group is the group of automorphisms of some object in some category. (§2.1]

Solution. Let G be a group with binary operation $\circ$ and identity e. Consider a category C with a single object $\emptyset$. We will show that the elements of G make suitable morphisms $\mathrm{Hom}_{\mathsf{C}}(\emptyset, \emptyset)$ with $\circ$ as a composition operation.

Since G is a group, G (i.e. $\mathrm{Hom}_{\mathsf{C}}(\emptyset, \emptyset)$) is closed $\circ$ and $\circ$ is transitive for morphisms. The identity e makes an appropriate identity morphism for $\emptyset$. Hence C is a category.

Lastly, we will show that C is a groupoid. Any morphism $f \in \mathrm{Hom}_{\mathsf{C}}(\emptyset, \emptyset)$ has a (two-sided) inverse f^{-1} since G is a group. This means that f is an isomorphism. □

Problem 1.2. Consider the 'sets of numbers' listed in §1.1, and decide which are made into groups by conventional operations such as $+$ and $\cdot$. Even if the answer is negative (for example, $(\mathbb{R}, \cdot)$ is not a group), see if variations on the definition of these sets lead to groups (for example, $(\mathbb{R}^*, \cdot)$ is a group; cf. §1.4). [§1.2]

Solution. This is open-ended, so I don't want to do it. □

Problem 1.3. Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h of a group G.

Solution. Let B be a group and suppose $f, g \in G$. Then we have:

$$(g^{-1}f^{-1})(fg) = (g^{-1}(f^{-1}f))g = (g^{-1}e)g = g^{-1}g = e$$

$$(fg)(g^{-1}f^{-1}) = (f(gg^{-1}))f^{-1} = (fe)f^{-1} = ff^{-1} = e$$

Hence $g^{-1}f^{-1}$ is a two-sided inverse of gf. □

Problem 1.4. Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

Solution. Let G be a group such that for all $g \in G$ we have $g^2 = e$. Fix $g, h \in G$. Then,

$$gh = eghe = hhghgg = h(hg)^2g = hg$$

as required. □

Problem 1.5. The 'multiplication table' of a group is an array compiling the results of all multiplications $g \bullet h$:

[Redacted.]

(Here e is the identity element. Of course the table depends on the order in which the elements are listed in the top row and leftmost column.) Prove that every row and every column of the multiplication table of a group contains all elements of the group exactly once (like Sudoku diagrams!).

Solution. Without loss of generality suppose that two elements in a column are different, i.e. for some fixed element f we have $f \bullet g = f \bullet h$. Then by (left-)cancellation we get that $g = h$. Hence the columns must be the same. □

Problem 1.6. ¬ Prove that there is only one possible multiplication table for G if G has exactly 1, 2, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are two distinct tables, up to reordering the elements of G. Use these tables to prove that all groups with < 4 elements are commutative.

(You are welcome to analyze groups with 5 elements using the same technique, but you will soon know enough about groups to be able to avoid such brute-force approaches.) [2.19]

Solution. (Note: I spent a lot of time trying to figure out why there seemed to be many more than 2 tables for groups with exactly 4 elements until going back to the question where it there are only 2 "up to reordering"!)

If a group only has one element, say $G = \{ e \}$, there is only one spot to fill. Since multiplication must be closed it must be e. Here e is the identity.

If a group has two elements, say $G = \{ e, g \}$, then there are four spots to fill. The e-row and e-column are easy, so there is only one non-trivial column to fill. If $gg = g$ then by cancellation we get that $g = e$, which is a contradiction since g is distinct from e. So $gg = e$.

Suppose that $G = \{ e, g, h \}$. Here there are four non-trivial spots to fill. We can't have that $gh = h$ (by cancellation as above), so we must have $gh = e$. For the same reason, we must have $hg = e$. There is no other choice but to set $g^2 = h$ and $h^2 = g$.

Suppose that $G = \{ e, f, g, h \}$. This is the tricky one. There are nine spots to fill. First of all, we note that due to the double-sidedness of inverses, we have that for $f, g, h \in G$ (all distinct) we can't have that $fg = h$ and $gf = e$ (the second implies that $f = g^{-1}$, but then the first says $g^{-1}g \neq e$, a contradiction.) This in fact implies commutativity, since for any distinct $f, g \in G$ it must either be the case that $fg = e = gf$ or $fg = h = gf$.

The question states that there are only two "up to the order of the elements". So, rather than answer "how many possible tables are there", we will answer: how many n are such that n elements of G go to the identity when squared? We'll see that only $n = 1$ and $n = 3$ work; and that the only differences in the tables for $n = 1$ are the choosing of which element has order 2 (i.e. which element goes to the identity when it is squared;) and that there is only one table where $n = 3$.

Clearly it can't work for $n < 0$ or $n > 3$ (we can't choose less than 0 or more than 3 elements from G.) We claim that it can't be that no element in G has order 2. To see this, without loss of generality consider f. We know that f must have an inverse that is distinct from itself (or else we get an immediate contradiction) and from e—without loss of generality, suppose $f^{-1} = h$. This also means that $h^{-1} = f$. Now we ask: which element can be the inverse of g? It can't be f or h because the inverse is unique and g is distinct from f and h. It also can't be e since $ge = g$ by definition. So it must be g. But this means that there are 1 elements that have order 2. We have shown that, if any element in G doesn't have order 2, another must have order 2. So zero order two elements is a contradiction.

Now we claim that having only two elements of order not equal to 2 is also infeasible. Assume without loss of generality that $f^2 = e$ and $g^2 = e$. What is h^2? We note that the inverse of h cannot be e by cancellation, and cannot be f or g since inverses are unique and h is distinct from f and g. This means that h must be its own inverse, and thus has order 2. Therefore, two elements of order 2 implies three elements of order 2.

Now we'll show that one order 2 element works okay. Without loss of generality assume $f^2 = e$. Here we must take $gh = hg = e$. These are three cells in our table. Furthermore, we must have $fg = h$ (since fg can't be f or g or e), and similarly for $fh = g$. By commutativity we also have that $gf = h$ and $hf = g$. Now we've filled seven cells in our table. By our above "theorem" about column and row uniqueness we know we must take $gh = hg = f$. Hence there is only one group of size 4 with only one order 2 element (up to the selection of which element has order 2.)

Last, consider the group of size 4 where all elements are order 2. Immediately we deducate that $fg = h$ (since it can't be e, f, or g by cancellation,) and then that $fh = g$ (since it is the last option!) Similarly that $gh = f$, and so on—there is only one group where all elements are order 2. □

Problem 1.7. Prove Corollary 1.11.

Solution. Too easy: $|g|$ is a divisor of n is equivalent to n is a multiple of $|g|$. □

Problem 1.8. Let G be a finite group, with exactly one element f of order 2. Prove that $\prod_{g\in G} g = f$. [4.16]

Solution. I struggled a lot with this problem. The question implies that $\prod_{g\in G}$ is well-defined, which means that G is a commutative group, however I could not prove this.

Assuming that it is commutative, then we can take $G = \left\{ e, f, g_1, \dots, g_m, g_1^{-1}, \dots, g_m^{-1} \right\}$ all distinct. Then the product $\prod_{g\in G}$, since G is commutative, can be written $efg_1g_1^{-1}\cdots g_mg_m^{-1} = efe\cdots e = f$ as required.

(I hope to figure out how to prove that G is commutative eventually.) □

Problem 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, n, m as above. Note that every element $g \in G$ that is not e and is not order 2 has a unique inverse g^{-1} such that $g \neq g^{-1}$. Hence every element except for e and except for all the order 2 elements come in pairs; there are, say $2k$ of them. Then $n = 1 + m + 2k$, where the 1 corresponds to e, m is the number of order-2 elements, and k is the number of pairs g, g^{-1}. It follows that $n - m = 2k + 1$, so $n - m$ is odd.

Further, suppose n is even, so $n = 2p$ for some p with $p > k$ (for the $2k$ elements doesn't include the identity element e, there must be more than $2k$ elements in G, i.e. $2p > 2k$, which implies $p > k$.) Then $n = 2p = 1 + m + 2k$. Rearranging we get that $m = 2(p - k) - 1$. Since $p > k$, $p - k \geq 1$, so $2(p - k) \geq 2$, and $2(p - k) - 1 \geq 1$, hence $m \geq 1$ so G necessarily contains at least one element of order 2. □

Problem 1.10. Suppose the order of g is odd. What can you say about the order of g^2?

Solution. Suppose $|g| = 2k + 1$ for some k. Then, by Proposition 1.13,

$$\left|g^2\right| = \frac{\operatorname{lcm}(2, 2k+1)}{2} = \frac{4k+2}{2} = 2k + 1$$

(where we take $\operatorname{lcm}(2, 2k+1) = 2(2k+1)$ since $2k+1$, being odd, is relatively prime with 2.) Hence $\left|g^2\right| = |g|$. □

Problem 1.11. Prove that for all g, h in a group G, $|gh| = |hg|$. (Hint: Prove that $\left|a^{-1}ga\right| = |g|$ for all a, g in G.)

Solution. Let $g, a \in G$. Suppose $|g| = n$. Then,

$$(a^{-1}ga)^n = (a^{-1}ga)(a^{-1}ga)\cdots(a^{-1}ga) = a^{-1}g(aa^{-1})g\cdots g(aa^{-1})ga = a^{-1}g^n a$$

We also have that $g^n = e \iff g^n = aa^{-1} \iff a^{-1}g^n a = e$. This means that $\left|a^{-1}ga\right| = n = |g|$, which implies that $|ag| = \left|aa^{-1}ga\right| = |ga|$, as required. □

Problem 1.12. I don't want to typeset the matrices!

Problem 1.13. $\triangleright$ Give an example showing that $|gh|$ is not necessarily equal to $\operatorname{lcm}(|g|, |h|)$, even if g and h commute. [1.6, 1.14]

Solution. Consider the 4-group with 1 element of order two as above. Then we have $G = \{\, e, f, g, h \,\}$ with $f^2 = e$, $gh = hg = e$, and $g^2 = h^2 = f$. Here we have that $|gh| = |e| = 0$, while $\operatorname{lcm}(|g|, |h|) = \operatorname{lcm}(4, 4) = 4$, so $|gh| \neq \operatorname{lcm}(|g|, |h|)$. □

Problem 1.14. $\triangleright$ As a counterpoint to Exercise 1.13, prove that if g and h commute and $\gcd(|g|, |h|) = 1$, then $|gh| = |g|\,|h|$. (Hint: Let $N = |gh|$; then $g^N = (h^{-1})^N$. What can you say about this element?) [§1.6, 1.15, §IV.2.5]

Solution. Let $g, h \in G$ with $gh = hg$. Set $|g| = n$, $|h| = m$, and $|gh| = |hg| = N$. Suppose that $\gcd(n, m) = 1$. We have by Proposition 1.14 that $N \mid \operatorname{lcm}(n, m)$. Since $\gcd(n, m) = 1$, $\operatorname{lcm}(n, m) = nm$. So $nm = kN$ (1) for some k. Also, since $\gcd(n, m) = 1$ we get that $N \mid n$ xor $N \mid m$. Suppose, without loss of generality, that $N \mid n$, so that $n = \ell N$ for some ℓ (2). Divide (1) by (2) to get that $m = \frac{k}{\ell}$ (3). Now, we will prove that $k = 1$. Since $(gh)^N = g^N = e$, we get that $g^N = (h^{-1})^N$ (4). By (2) we get that $\left|g^N\right| = \ell$. Since $h^m = e$, we have $hh^{m-1} = e$, so $h^{-1} = h^{m-1}$. By (4) we know that $\left|(h^{m-1})^N\right| = \left|h^{N(m-1)}\right| = \ell$. However, by Proposition 1.13 we know that $\ell = \frac{\operatorname{lcm}(m,N(m-1))}{N(m-1)}$. Since $N \mid nm$ and $\gcd(n, m) = 1$ and we're assuming $N \mid n$, $\gcd(N, m) = 1$. So $\ell = \frac{m(N(m-1))}{N(m-1)} = m$. From this we get $m = \frac{k}{\ell} = \frac{k}{m} \implies k = 1$. Looking back at (1) where $nm = kN$ we can finally deduce that $nm = N$. □

Problem 1.15. $\neg$ Let G be a commutative group, and let $g \in G$ be an element of maximal finite order, that is, such that if $h \in G$ has finite order, then $|h| < |g|$. Prove that in fact if h has finite order in G, then $|h| \mid |g|$. (Hint: Argue by contradiction. If $|h|$ is finite but does not divide $|g|$, then there its a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s coprime to p and $m < n$. Use Exercise 1.14 to compute the order of $g^{p^m} h^s$.) [§2.1, 4.11, IV.6.15]

Solution. TODO □