Aluffi - Algebra: Chapter 0

Chapter 2: Groups, First Encounter

October 4, 2018

1 Definition of a Group

Exercise 1.1. Consider a group G, and define C by $\mathrm{Obj}(\mathsf{C}) = \{X\}$, a singlet, and $\mathrm{Hom}_{\mathsf{C}}(X, X) = (G, \cdot)$, where $\cdot$ is the group product on G. Then by the group axioms we have an associative notion of composition in C with $e \in G$ the identity with respect to this. Therefore C is a category. Furthermore, any $g \in G$ has an inverse $g^{-1} \in G$, so all the $g \in \mathrm{Hom}_{\mathsf{C}}(X, X)$ are isomorphisms. Then C is a groupoid. So any group is the group of isomorphisms of a groupoid.

Exercise 1.2. In the following, $a, b, d, c \in \mathbb{R}$, $m, n, p, q \in \mathbb{Z}$. Addition and multiplication are both associative, and the respective identities are 0 and 1, resp.

(i) $(\mathbb{Z}, +)$: $m + n \in \mathbb{Z}$; m has the inverse $-m$. This is a group

(ii) $(\mathbb{Z}, \cdot)$: $m \cdot n \in \mathbb{Z}$; m only has an inverse in $\mathbb{Z}$ if $m = \pm 1$. So $(\mathbb{Z}, \cdot)$ is not a group. Consider instead $(\{\pm 1\}, \cdot)$: this is still closed, and has inverses, so this is a group.

(iii) $(\mathbb{Q}, +)$: $p/q + m/n = (pn + mq/qn) \in \mathbb{Q}$; p/q has the inverse $-p/q$. This is a group.

(iv) $(\mathbb{Q}, \cdot)$: $p/q \cdot m/n = pm/qn \in \mathbb{Q}$; p/q has the inverse q/p. This is a group.

(v) $(\mathbb{R}, +)$: $a + b \in \mathbb{R}$; a has the inverse $-a$. This is a group.

(vi) $(\mathbb{R}, \cdot)$: $a \cdot b \in \mathbb{R}$; a has the inverse $1/a$, unless $a = 0$, so this is not a group. Consider instead $(\mathbb{R}\backslash\{0\}, \cdot)$: this is still closed, and has inverses, so this is a group.

(vii) $(\mathbb{C}, +)$: $(a + ib) + (c + id) = (a + c) + i(b + d) \in \mathbb{C}$; $a + ib$ has the inverse $-a - ib$. This is a group.

(viii) $(\mathbb{C}, \cdot)$: $(a + ib)(c + id) = (ac - bd) + i(ad + bc) \in \mathbb{C}$; $a + ib$ has the inverse $1/(a + ib) = (a - ib)(a^2 + b^2)$, unless $a = b = 0$, so this is not a group. Consider instead $(\mathbb{C}\backslash\{0\}, \cdot)$: this is still closed and has inverses, so this is a group.

Exercise 1.3. We have $(gh)(h^{-1}h^{-1}) = e$, and inverses are unique, so $(gh)^{-1} = h^{-1}g^{-1}$.

Exercise 1.4. $g^2 = e$ for all $g \in G$. Then $g^{-1} = g$ for all g, so $(gh)^{-1} = gh$. But by the previous question, $(gh)^{-1} = h^{-1}g^{-1} = hg$, so $gh = hg$ and the group is commutative.

Exercise 1.5. Suppose h appears twice in the row of the element g, at the columns of h' and h''. Then $gh' = gh'' = h$. But then $g^{-1}gh' = g^{-1}gh'' = g^{-1}h$, so $h' = h''$, and so in fact it only appears once. Furthermore, for any $h \in G$, $g^{-1}h \in G$, and h appears in this column. The same is true for columns. Therefore each element appears exactly once in each row and column of the multiplication table.

Exercise 1.6.

(i) If $|G| = 1$, $G = \{e\}$ and the multiplication table is trivial and G is commutative.

(ii) If $|G| = 2$, $G = \{e, g\}$, and by the previous question there is only one possible multiplication table

$\cdot$	e	g
e	e	g
g	g	e

(iii) If $|G| = 3$, $G = \{e, g, h\}$, and again there is only one possible multiplication table

$\cdot$	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

(iv) If $|G| = 4$, $G = \{e, g_1, g_2, g_3\}$. We have to have

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1			
g_2	g_2			
g_3	g_3			

If $g_1^2 = e$, then this becomes

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_3	g_2	
g_2	g_2			
g_3	g_3			

The remaining entries are either

$$\begin{matrix} e & g_1 \\ g_1 & e \end{matrix}$$

or with g_1 and e reversed. These two choices amount to relabelling g_2 and g_3, and either way the table is symmetric so G is Abelian. If instead $g_1^2 = g_2$ (or g_3, which is just a relabelling), then the entire table is fixed.

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3	e	g_1
g_3	g_3	e	g_1	g_2

This is also commutative.

Therefore we have that, up to relabelings, group structure is fixed for $|G| \leq 3$, there are exactly two possible structures for $|G| = 4$, and for $|G| \leq 4$, G is Abelian.

Exercise 1.7. Consider an element $g \in G$ of finite order. By Lemma 2.10, $g^N = e$, so $|g|$ divides N, and hence $N = n|g|$ for some positive integer n. Conversely, if $|g|$ divides N, $n|g| = N$ for some positive integer N, so $g^N = g^{n|g|} = (g^{|g|})^n = e^n = e$.

Exercise 1.8. Consider a group $G = \{e, f, g_i\}$, with $|f| = 2$ and $|g_i| \neq 2$. $\prod_{g \in G} g$ is defined so G is Abelian. Since $f^{-1} = f$, the inverse of any of the g_i is some g_j, and since $|g_i| \neq 2$, $i \neq j$. Thus $\prod_i g_i = e$. Then $\prod_{g \in G} = eef = f$.

Exercise 1.9. Let $|G| = n$, and m be the number of elements of G of order 2. If $|g| = 2$, $g^{-1} = g$. There are $n - m - 1$ elements with $|g| > 2$, since e is the only element of order 1. These $n - m - 1$ must have inverses among themselves, and they must be distinct from their inverses, since their order is more than 2. Then they can be paired off, and hence $n - m - 1$ is even, so $n - m$ is odd.

If furthermore n is even, m is odd, so at least 1.

Exercise 1.10. Consider an element $g \in G$ of order n, where n is odd. By Proposition 1.13,

$$|g^2| = \frac{\operatorname{lcm}(2,n)}{2}$$

Since n is odd, $\operatorname{lcm}(2,n) = 2n$, so $|g^2| = n = |g|$.

Exercise 1.11. Let $|gh| = n$. Then

$$\begin{aligned}
(gh)^n &= e \\
g^{-1}(gh)^n h^{-1} &= g^{-1}h^{-1} \\
(hg)^{n-1} &= g^{-1}h^{-1} \\
(hg)^n &= g^{-1}h^{-1}hg = e \\
\Rightarrow |hg| &= n = |gh|
\end{aligned}$$

Exercise 1.12. Consider $G = GL(\mathbb{R}^2)$, and

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Then

(i) $g^2 = -\operatorname{id}$, so $g^3 = -g$ and $g^4 = \operatorname{id}$, so $|g| = 4$.

(ii)

$$h^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

so $h^3 = \operatorname{id}$.

(iii) We calculate

$$\begin{aligned}
gh &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
(gh)^2 &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
(gh)^3 &= \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

so we see that

$$(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

so $|gh| = \infty$.

Exercise 1.13. Suppose $|G| = 4$ and exactly one element is of order 2. Write $G = \{e, f, g, h\}$, with $|f| = 2$. Then $f^2 = e$ and $gh = hg = e$, so $g^2 = h^2 = f$. Then $|gh| = 0$ but lcm$(|g|, |h|)$ =lcm$(4, 4) = 4$.

Exercise 1.14. Suppose $gh = hg$, and let $n = |g|$, $m = |h|$, $N = |gh|$, and $\gcd(n, m) = 1$. By Proposition **??**, N divides lcm$(n.m)$. Since $\gcd(n, m) = 1$, lcm$(n, m) = nm$, so $nm = kN$ for some integer k, and hence N divides either n or m. WLOG suppose N divides n. Then $n = lN$ for some integer l, and hence $m = k/l$. Now, $(gh)^N = g^N = e$, so $g^N = h^{-N}$. Since $n = lN$, $|g^N| = l$. Since $h^m = e$, $h^{-1} = h^{m-1}$, and since $h^{\scriptscriptstyle N} = g^N$, $|(h^{m-1})^N| = l$. However, by Proposition **??**,

$$l = \frac{\text{lcm}(m, N(m-1))}{N(m-1)}$$

Since N divides n and $\gcd(n, m) = 1$, $\gcd(N, m) = 1$. So

$$l = \frac{m(N(m-1))}{N(m-1)} = m$$

So $m = k/l = k/m$ and hence $k = 1$. Thus $nm = N$.

Exercise 1.15. Let G be commutative, and $g \in G$ have the largest order out of those elements of G of finite order. Suppose $|h| = n$ does not divide $|g| = m$. Then $n > 1$, and there exists a prime p such that $m = p^k r$, $n = p^l s$ for $0 \leq k \leq l$ and $\gcd(p, r)$ =$\gcd(p, s) = 1$. Consider $g^{p^k} h^s$. By Proposition **??**,

$$|g^{p^k}| = \frac{\text{lcm}(p^k, m)}{p^k} = \frac{m}{p^k} = r$$
$$|h^s| = \frac{\text{lcm}(s, n)}{s} = \frac{n}{s} = p^l$$

so by Exercise 1.14, by the commutativity of G and $\gcd(r, p^l) = 1$, $|g^{p^k} h^s| = rp^l$. But $k < l$, so $|g| = m = p^k r < p^l r$, and $|g|$ is not maximal, contrary to hypothesis. Then for all primes p, its multiplicity in the factorisation of $|g|$ must be greater than that of $|h|$, i.e. $k \geq l$ for all primes. So $|h|$ divides $|g|$.

2 Examples of Groups

Exercise 2.1. Define a representation $R : S_n \to GL(\mathbb{R}^n)$ by $R(\sigma) = M$, where $M_{ij} = \delta_{j,\sigma(i)}$. Then if $R(\sigma) = M$ and $R(\tau) = N$, then

$$\begin{aligned} M_{ij}N_{jk} &= \delta_{j,\sigma(i)}\delta_{k,\tau(j)} \\ &= \delta_{k,\tau(\sigma(i))} \end{aligned}$$

so write $MN = R(\sigma')$, where

$$\sigma' = \begin{pmatrix} 1 & 2 & ... & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & ... & \tau(\sigma(n)) \end{pmatrix}$$

But this is just $\sigma \cdot \tau$, so

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

Exercise 2.2. Consider $\sigma \in S_n$. If $|\sigma| = 1$, $\sigma = e$. If $|\sigma| = 2$, σ swaps two elements. In this fashion it is easy to see that if σ cycles d elements, then $|\sigma| = d$. Since such permutations exist for all $d \leq n$, elements of order d exist for all $d \leq n$.

Exercise 2.3. As per the previous question, a permutation which cycles n out of N elements is order n.

Exercise 2.4. Label the vertices of a square 1, 2, 3, 4, in clockwise. Then consider

$D_8 = \{R_{n\pi/2}, R'_{n\pi/2} \mid n = 0,1,2,3\}$, where R'_θ includes a reflection. Define $f : D_8 \to S_4$ by

$$\begin{aligned}
R_0 = e \mapsto e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
R_{\pi/2} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\
R_{\pi} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\
R_{3\pi/2} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\
R'_0 \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
R'_{\pi/2} = R'_0 \cdot R_{\pi 2} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\
R'_{\pi} = R'_0 \cdot R_{\pi} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
R'_{3\pi/2} = R'_0 \cdot R_{3\pi/2} \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}
\end{aligned}$$

Clearly this is a homomorphism.

Exercise 2.5. Consider the n-gon, and its group of symmetries, D_{2n}. This group has generators x and y, where x is a reflection, and y a rotation by $2\pi/n$, so clearly $x^2 = e$ and $y^n = e$. We can also see that $yx = xy^{-1}$, so $y^2x = yxy^{-1} = xy^{-2}$, and so on, and hence $y^r x = xy^{-r}$. Then consider a generic element

$$\begin{aligned}
x^{i_1}y^{i_2}x^{i_3}y^{i_4}... &= \begin{cases} xy^{i_2}x^{i_3}y^{i_4}... & i_1 \text{ odd} \\ y^{i_2}x^{i_3}y^{i_4}... & i_1 \text{ even} \end{cases} \\
&= \begin{cases} y^{-i_2}x^{1+i_3}y^{i_4}... & i_1 \text{ odd} \\ y^{i_2-i_4}x... & i_1 \text{ even, } i_3 \text{ odd} \\ y^{i_2+i_4}... & i_1 \text{ even, } i_3 \text{ even} \end{cases}
\end{aligned}$$

and so on. In this fashion we see that the three relations stated can reduce any such combination to $x^i y^j$ for some $i = 0, 1$, $j = 0, ..., n-1$.

Exercise 2.6. Suppose g and h are two elements of a group both of order 2, i.e. $g^{-1} = g$ and $h^{-1} = h$.

(i) If $|gh| = 1$, $gh = e$, so $g^{-1} = h$ and by the uniqueness of inverses, $g = h$. So then we have this for any group including an element of order two, such as D_6, with g a reflection.

(ii) If $|gh| = n > 1$, let g and h be reflections in D_{2n} around different axes, which for simplicity we can take as $g = y^{n-1}x$ and $h = x$. Then indeed

$$g^2 = y^{n-1}xy^{n-1}x = y^0x^2 = e$$

and clearly $h^2 = e$. Then,

$$gh = y^{n-1}x^2 = y^{n-1} = y^{-1}$$

so if $(gh)^m = e$, $y^{-m} = e$, and the smallest such m for which this is true is precisely n. Therefore D_{2n} has two elements of order 2 such that the order of their product is n.

Exercise 2.7. An element $g \in D_{2n}$ is in the centre of D_{2n}, $Z(D_{2n})$ iff it commutes with both x and y. By Exercise, we can write $g = x^iy^j$, where $i = 0, 1$ and $j = 0, ..., n-1$. Then if g commutes with y, $x^iy^j = yx^iy^j$, so $x^iy = yx^i$. If $i = 1$ we have $xy = yx$, but we know that $yx = xy^{-1}$, so we would then have that $xy = xy^{-1}$, i.e. that $y = y^{-1}$, which is not the case. Therefore $i = 0$, and $g = y^j$. If this also commutes with x, we have $y^jx = xy^j = y^{n-j}x$, which requires $j = n - j$. This is only possible if j is zero, in which case $g = e$, or n is even, and then $g = y^{n/2}$. Thus

$$Z(D_{2n}) = \begin{cases} \{e\} & n \text{ odd} \\ \{e, y^{n/2}\} & n \text{ even} \end{cases}$$

Exercise 2.8. Consider the five platonic solids.

(i) The faces of a tetrahedron are triangles, i.e. minimal polygons, so by labelling each face from 1 to 4, we must have that every permutation $\sigma \in S_4$ corresponds to a symmetry of the tetrahedron (just as $D_6 \cong S_3$), and indeed there are no further symmetries. Thus the dihedral group of the tetrahedron is of the order $|S_4| = 24$.

(ii) Consider the cube, and assign a number to each pair of opposite vertices. These can be permuted in any order, so we have S_4 describing the rotational symmetries, of which there are 24. Then there must be a further 24 symmetries involving a reflection, so in total 48 symmetries.

(iii) The octahedron is the dual of the cube, so we can make the same argument, but with faces in the place of vertices.

(iv) The faces of the dodecahedron are pentagons, which have an odd and non-minimal number of sides, and hence we have $|A_5| = 60$ rotational symmetries, and another 60 involving a reflection, so a total of 120.

(v) The icosahedron is the dual of the dodecahedron, so also has 120 symmetries.

Exercise 2.9. We define congruence mod n by $a \equiv b \mod n$ iff $a - b \in n\mathbb{Z}$.

(i) $a - a = 0 \in n\mathbb{Z}$ so $a \equiv a \mod n$.

(ii) If $a - b \in n\mathbb{Z}$, so is $b - a$, so $a \equiv b \mod n$ implies $b \equiv a \mod n$.

(iii) If also $b - c \in n\mathbb{Z}$, so is $a - c = (a - b) + (b - c)$, so $a \equiv b \mod n$ and $b \equiv c \mod n$ imply $a \equiv c \mod n$

Therefore this is an equivalence relation.

Exercise 2.10. For given $n \in \mathbb{Z}$, any integer can be written $kn + r$ for $0 \leq r < n$ and some integer k. Thus

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, ..., [n-1]_n\}$$

Exercise 2.11. Let $n \in \mathbb{Z}$, so $2n - 1$ is odd. Consider $(2n-1)^2 - 1 = 4n(n-1)$. Then

$$\frac{(2n-1)^2 - 1}{8} = \frac{1}{2}n(n-1)$$

On the LHS, either n or $n - 1$ is even, so the RHS is an integer, and hence the square of any odd number is congruent to 1 mod 8.

Exercise 2.12. Consider the equation

$$a^2 + b^2 = 3c^2$$

where $a, b, c \in \mathbb{Z}$. In $\mathbb{Z}/4\mathbb{Z}$, this is

$$[a]_4^2 + [b]_4^2 = 3[c]_4^2$$

i.e.

$$[a^2 + b^2]_4 = [3c^2]_4$$

Therefore $a^2 + b^2 - 3c^2 \in 4\mathbb{Z}$. Either none of a, b, c are odd or two are. Suppose a and b are odd. Then write $a = 2n - 1$, $b = 2m - 1$, so

$$a^2 + b^2 = 4(n^2 - n + m^2 - m) + 2$$

Then we would have to have $3c^2$ be even, but not a multiple of four. But c^2 is only even if c is, in which case it is a multiple of four. So we cannot have a and b odd. Suppose instead a and c are odd, with $a = 2n - 1$ again and $c = 2m - 1$ this time. Then

$$a^2 - 3c^2 = 4(n^2 - n - 3m^2 + 3m) - 2$$

This would require b^2 to be even but not a multiple of four, which again is not possible. So we cannot have a and c odd, and by the same token we cannot have b and c odd. Therefore we must have all a, b, c even. Then we can write $a = 2k$, $b = 2l$, $c = 2m$ for integers k, l, m. Then we have

$$k^2 + l^2 = 3m^2$$

This is just the original equation. Therefore we can proceed by continuing to divide our unknowns by two until they cease to be even, which must happen in finitely many steps working in $\mathbb{Z}/4\mathbb{Z}$. Then we reach a contradiction, and therefore there is no solution to this equation in the integers.

Exercise 2.13. Suppose $\gcd(m, n) = 1$. Then by Corollary 2.5, $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$, so any $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ may be written $[b]_n = a[m]_n$ for some integer a. In particular, $a[m]_n = [1]_n$ for some integer a, so $am - 1 = b'n$ for some b', i.e. $am - b'n = 1$. Let $b = -b'$, and then we have $am + bn = 1$.
Conversely, suppose $am + bn = 1$ for some integers a and b. Suppose there exists a prime p such that $m = pr$ and $n = ps$, so $\gcd(m, n) \geq p > 1$. Then $am+bn = 1$ reads $p(ar+bs) = 1$, but $ar + bs \in \mathbb{Z}$, and no prime is the reciprocal of an integer, so this is false. Therefore we must have $\gcd(m, n) = 1$.
Thus, $\gcd(m, n) = 1$ iff there exist integers a and b such that $am + bn = 1$.

Exercise 2.14. From the product on $\mathbb{Z}$ we have an induced notion of a product on $\mathbb{Z}/n\mathbb{Z}$ given by

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

Suppose $a' - a = kn$, $b' - b = ln$ for integers k, l. Then

$$a' \cdot b' - a \cdot b = n(kln + kb + al)$$

so n divides $a' \cdot b' - a \cdot b$. Thus this induced product is well-defined.

Exercise 2.15. Let $n > 0$ be odd.

(i) Suppose $\gcd(2m+n, 2n) = d > 1$, i.e. that $d \mid 2m+n$ and $d \mid 2n$. By the first of these, d is odd. By this oddness and the second, $d \mid n$. Then also $d \mid 2m$ and so $d \mid m$. Then $\gcd(m, n) \geq d > 1$, but if $\gcd(m, n) - 1$ this is false, so in fact $\gcd(2m + n, 2n) = 1$.

(ii) If $\gcd(r, 2n) = 1$, there exist by Exercise 2.13 integers $a, b \in \mathbb{Z}$ such that $ar + 2bn = 1$. Then let $a' = 2a \in \mathbb{Z}$ and $b' = 2b - a \in \mathbb{Z}$. We then have

$$a' \frac{r+n}{2} + b'n = 1$$

so again by Exercise 2.13,

$$\gcd\left(\frac{r+n}{2}, n\right) = 1$$

(iii) Define $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$ by $f([m]_n) = [2m + n]_{2n}$. Firstly, by the first part of this exercise, $[2m + n]_{2n}$ is indeed in $(\mathbb{Z}/2n\mathbb{Z})^*$ for $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ and n odd. Then,

$$f([m + n]_n) = [2m + 3n]_{2n} = [2m + n]_{2n}$$

so f is well-defined. Then, suppose $[2m + n]_{2n} = [2m' + n]_{2n}$. Then $2m - 2m' \in 2n\mathbb{Z}$, so $m - m' \in n\mathbb{Z}$, so $[m]_n = [m']_n$, so f is injective. Lastly, consider $[r]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. $\gcd(r, 2n) = 1$, so by the second part of this exercise, $\gcd((r + n)/2, n) = 1$, so we have the element $[(r + n)/2]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, and hence we can write

$$f\left(\left[\frac{r+n}{2}\right]_n\right) = [r + 2n]_{2m}$$

so f is surjective. Therefore f is a bijection.

Exercise 2.16. Consider $1238237^{18238456}$. In $\mathbb{Z}/10\mathbb{Z}$, we have $[1238237]_{10} = [7]_{10}$. Noting that $18238237 = 4 \times 4559614$, we consider

$$[1238237]_{10}^4 = [7]_{10}^4 = [7^2]_{10}^2 = [9]_{10}^2 = [1]_{10}$$

and hence

$$[1238237]_{10}^{18238456} = [1]_{10}^{4559614} = [1]_{10}$$

Thus the last digit of $1238237^{18238456}$ is 1.

Exercise 2.17. Let $m \equiv m' \mod n$, so $(m - m')/n = p \in \mathbb{Z}$.
$\Rightarrow$ Suppose $\gcd(m, n) = 1$. Then by Exercise 2.13 there exist integers a and b such that $am + bn = 1$. Let $a' = a$ and $b' = b + ap$. Then this reads $a'm + b'n = 1$, so $\gcd(m', n) = 1$.
$\Leftarrow$ The converse is obtained by following the same steps in reverse.

Exercise 2.18. Let $d \leq n$, and define a map $f : \mathbb{Z}/d\mathbb{Z} \to S_n$ which takes $[a]_d$ to the permutation cycling the first d elements by a places. This is well-defined, since cycling d elements an extra nd times has no effect for any integer n. Similarly it is injective. Furthermore, it is a homomorphism, since $f([a]_d + [b]_d) = f([a + b]_d)$ cycles the d elements $a + b$ times, which is equivalent to cycling them a times followed by b times.

Exercise 2.19. Consider

$$(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

Instead of calculating the whole multiplication table, we can just consider the squares of each non-trivial element. We have $[2]_5^2 = [4]_5$, $[3]_5^2 = [4]_5$, and $[4]_5^2 = [1]_5$, so only one element of order 2. Now consider

$$(\mathbb{Z}/12\mathbb{Z})^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$$

and $[5]_{12}^2 = [1]_{12}$, $[7]_{12}^2 = [1]_{12}$, and $[11]_{12}^2 = [1]_{12}$, so three elements of order 2. Therefore these two groups cannot be the same up to relabeling.

3 The Category Grp

Exercise 3.1. Let $\phi : G \to H$ be a morphism in C, a category with products. Then for any Z and choices $f_H, f'_H : Z \to H$ there is a unique morphism $\psi : Z \to H \times H$ making

$$\begin{tikzcd}
 & & H \\
Z \arrow[r, "\psi"] \arrow[urr, bend left, "f_H"] \arrow[drr, bend right, "f'_H"'] & H \times H \arrow[ur, "\pi_{H1}"] \arrow[dr, "\pi_{H2}"] & \\
 & & H
\end{tikzcd}$$

commute. In particular, consider $Z = G \times G$, $f_H = \phi \cdot \pi_G$, $f'_H = \phi \cdot \pi'_G$. Then we must have

$$\begin{aligned}
\pi_{H1} \cdot \psi(g_1, g_2) &= \phi \cdot \pi_{G1}(g_1, g_2) = \phi(g_1) \\
\pi_{H2} \cdot \psi(g_1, g_2) &= \phi \cdot \pi_{G2}(g_1, g_2) = \phi(g_2)
\end{aligned}$$

so ψ is uniquely given by $\psi = \phi \times \phi$.

Exercise 3.2. Let $\phi : G \to H$ and $\psi : H \to K$ be morphisms in a category with products. Then as per the previous question we also have morphisms $\phi \times \phi$ and $\psi \times \psi$. We have the commuting diagram

$$\begin{tikzcd}
 & & H \arrow[rr, "\psi"] & & K \\
G \times G \arrow[r, "\phi\times\phi"] \arrow[urr, bend left, "\phi\cdot\pi_{G1}"] \arrow[drr, bend right, "\phi\cdot\pi_{G2}"] & H \times H \arrow[ur, "\pi_{H1}"] \arrow[dr, "\pi_{H2}"] \arrow[rr, "\psi\times\psi"] & & K \times K \arrow[ur, "\pi_{K1}"] \arrow[dr, "\pi_{K2}"] & \\
 & & H \arrow[rr, "\psi"] & & K
\end{tikzcd}$$

So, in particular, the diagram

$$\begin{tikzcd}
 & & K \\
G \times G \arrow[r, "(\psi\phi)\times(\psi\phi)"] \arrow[urr, bend left, "\psi\cdot\phi\cdot\pi_{G1}"] \arrow[drr, bend right, "\psi\cdot\phi\cdot\pi_{G2}"] & K \times K \arrow[ur, "\pi_{K1}"] \arrow[dr, "\pi_{K2}"] & \\
 & & K
\end{tikzcd}$$

commutes, and so $(\psi\phi) \times (\psi\phi) = (\psi \times \psi)(\phi \times \phi)$.

Exercise 3.3. Let G, H be Abelian groups. If $G \times H$ is their coproduct in Ab, for any Abelian group Z and choice of homomorphisms $\phi_G : G \to Z$ and $\phi_H : H \to X$, there is a unique $\psi : G \times H \to Z$ making

$$\begin{tikzcd}
G \arrow[dr, hook, "\iota_G"] \arrow[drr, bend left, "\phi_G"] & & \\
 & G \times H \arrow[r, "\psi"] & Z \\
H \arrow[ur, hook, "\iota_H"] \arrow[urr, bend right, "\phi_H"] & &
\end{tikzcd}$$

commute. Define ψ by

$$\psi(g, h) = \phi_G(g)\phi_H(h)$$

This is fully specified by Z and ϕ_G and ϕ_H, and because Z is Abelian it is unique. Then

$$\begin{aligned}
\psi((g_1, h_1)(g_2, h_2)) &= \psi(g_1 g_2, h_1 h_2) \\
&= \phi_G(g_1 g_2)\phi_H(h_1 h_2) \\
&= \phi_G(g_1)\phi_G(g_2)\phi_H(h_1)\phi_H(h_2)
\end{aligned}$$

Since Z is Abelian, this is

$$\begin{aligned}\psi((g_1, h_1)(g_2, h_2)) &= \phi_G(g_1)\phi_H(h_1)\phi_G(g_2)\phi_H(h_2)\\ &= \psi(g_1, h_1)\psi(g_2, h_2)\end{aligned}$$

so ψ is a homomorphism, and therefore $G \times H$ does indeed meet the universal property to be the coproduct in Ab.

Exercise 3.4. We can construct a bijection between $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ by drawing a square spiral out from the origin that moves in integer steps parallel to the x and y axes. Calling this f, we have $f(0) = (0, 0)$, $f(1) = (1, 0)$, $f(2) = (1, 1)$, $f(3) = (0, 1)$, and so on. Since both groups are additive, and this construction amounts to counting integer steps, it is a homomorphism. Thus $\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}$.

Exercise 3.5. Suppose $\mathbb{Q}$ is the product of two groups. For $a/b \in \mathbb{Q}$, write (a, b). Then $(a, b) + (c, d)$ is the rational

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

which is not $(a + c, b + d)$, so this construction doesn't work.

Exercise 3.6. Treat S_3 as a group with two generators, x and y, and relations $x^2 = e$, $y^3 = e$, $yx = xy^2$.

(i) Define $f_2 : C_2 \to S_3$ by $f_2([a]_2) = x^a$ and $f_3 : C_3 \to S_3$ by $f_3([a]_3) = y^a$. Clearly these are injective and homomorphisms.

(ii) Suppose $C_2 \times C_3$ is a coproduct in Grp. Then there is a unique homomorphism $\psi : C_2 \times C_3 \to S_3$ making

$$\begin{tikzcd}
C_2 \arrow[dr, hook, "\iota_2"] \arrow[drr, bend left, "f_2"] & & \\
& C_2 \times C_3 \arrow[r, "\psi"] & S_3 \\
C_3 \arrow[ur, hook, "\iota_3"] \arrow[urr, bend right, "\phi_3"] & &
\end{tikzcd}$$

commute. Then ψ must satisfy

$$\psi([a]_2, [0]_3) = f_2([a]_2) = x^a$$
$$\psi([0]_2, [b]_3) = f_3([b]_3) = y^b$$

S_3 is not Abelian, so there are two possibilities for what this ψ might be.

- Define ψ by

  $$\psi([a]_2, [b]_3) = x^a y^b$$

  Then

  $$\begin{aligned}\psi(([a_1]_2, [b_1]_3)([a_2]_2, [b_2]_3)) &= \psi([a_1 + a_2]_2, [b_1 + b_2]_3)\\ &= x^{a_1+a_2} y^{b_1+b_2}\\ &= x^{a_1} x^{a_2} y^{b_1} y^{b_2}\end{aligned}$$

  so ψ is only a homomorphism if $x^{a_2} y^{b_1} = y^{b_1} x^{a_2}$ for all a_2, b_1, which is not the case. Therefore this construction fails.

- Define ψ by

  $$\psi([a]_2, [b]_3) = y^b x^a$$

  This fails in the same way.

Therefore no such homomorphism ψ exists, and $C_2 \times C_3$ is not a coproduct in Grp.

Exercise 3.7. $\mathbb{Z}$ has one generator, x, with no relations. Then regard $\mathbb{Z} * \mathbb{Z}$ as a group with two generators, x and y, and no relations. Similarly, C_n is a group with one generator, x', and the relation $x'^n = e$, so regard $C_2 * C_3$ as a group with two generators, x' and y' with relations $x'^2 = e$ and $y'^3 = e$. Note how this resembles the notion of a disjoint union, the coproduct in Set. Then, define $f : \mathbb{Z} * \mathbb{Z} \to C_2 * C_3$ by $f(x) = x'$ and $f(y) = y'$. This is clearly surjective. $f(xy) = x'y' = f(x)f(y)$, so it is also a homomorphism.

Exercise 3.8. Let G be a group with two generators, x and y, and relations $x^2 = e_G$ and $y^3 = e_G$. If G is the coproduct $C_2 * C_3$ in Grp, then, as in Exercise 3.6 there is a unique morphism $\psi : C_2 * C_3 \to S_3$ making

$$\begin{tikzcd}
C_2 \arrow[rd, "\phi_2"] \arrow[rrd, bend left, "f_2"] & & \\
& G \arrow[r, "\psi"] & S_3 \\
C_3 \arrow[ru, "\phi"] \arrow[rru, bend right, "\phi_3"] & &
\end{tikzcd}$$

commute. So again $\psi \cdot \phi_2([a]_2) = f_2([a_2])$ and $\psi \cdot \phi_3([a]_3) = f_3([a]_3)$. Any element of G can be written $x^{i_1} y^{i_2} x^{i_3} y^{i_4}$.... There is only one way to choose ψ such that it both satisfies the requirements and is a homomorphism:

$$\psi(x^{i_1} y^{i_2} ...) = \psi(x^{i_1})\psi(y^{i_2}) ... = f_2([i_1]_2) f_3([i_2]_3) ...$$

Then we have satisfied the universal property for G to be the coproduct $C_2 * C_3$ in Grp. Note that the difference between G and $C_2 \times C_3$, which we tried in Exercise **??** is that now we have introduced some way of making the elements ψ maps to x and y not commute, whereas in $C_2 \times C_3$ they were in different factors, so independent. Again, notice how this coproduct is similar to the disjoint union, the coproduct in Set.

Exercise 3.9. Let A, B, C be Abelian groups, and $\phi : A \to C$, $\psi : B \to C$ homomorphisms. The fibred product $A \times_C B$ is an Abelian group which, together with projections $\pi_A : A \times_C B \to A$, $\pi_B : A \times_C B \to B$, satisfy that, for any Abelian group Z and choice of homomorphisms $f : Z \to A$, $g : Z \to B$, there is a unique homomorphism σ making

$$\begin{tikzcd}
 & & A \arrow[dr, "\phi"] & \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & A \times_C B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"] & & C \\
 & & B \arrow[ur, "\psi"] &
\end{tikzcd}$$

commute.
???

4 Group Homomorphisms

Exercise 4.1. If m divides n, we can define a homomorphism $\pi^n_m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ making the diagram

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

commute, i.e. $\pi^n_m([a]_n) = [a]_m$. This is well-defined since, because $m \mid n$, $[n]_m = [0]_m$, so

$$\pi^n_m([a+n]_n) = [a+n]_m = [a]_m$$

We can easily confirm it is a homomorphism:

$$\pi^n_m([a]_n + [b]_n) = \pi^n_m([a+b]_n) = [a+b]_m = [a]_m + [b]_m$$

Exercise 4.2. Consider the homomorphism $\pi_2^4 \times \pi_2^4 : C_4 \to C_2 \times C_2$. This is an isomorphism iff the underlying set-function is a bijection. However, π_2^4 maps both $[0]_4$ and $[2]_4$ to $[0]_2$, so the present homomorphism maps both of these to $([0]_2, [0]_2)$, and is hence not bijective.

Exercise 4.3. Let G be a group of finite order n.
$\Rightarrow$ Suppose $G \cong \mathbb{Z}/n\mathbb{Z}$. The generator of $\mathbb{Z}/n\mathbb{Z}$, $[1]_n$, is of order n, so by Proposition 4.8, there is an element in G of order n.
$\Leftarrow$ Suppose $g \in G$ is of order n. Then since $|G| = n$, the set $\{e, g, g^2, ..., g^{n-1}\}$ must be G itself, i.e. g generates G. But then we can map $g^i \mapsto [i]_n$, which is clearly bijective and homomorphic, so $G \cong \mathbb{Z}/n\mathbb{Z}$.

Exercise 4.4. $\mathbb{Z}$ and $\mathbb{Q}$ are countable, whereas $\mathbb{R}$ is not, so the only possible bijection between these sets is $\mathbb{Z} \to \mathbb{Q}$. Suppose such a homomorphism, ϕ, exists. Then there exists some rational q such that $\phi(q) = 1$. $q/2$ is also a rational, so we also have

$$1 = \phi(q) = \phi\left(\frac{q}{2} + \frac{q}{2}\right) = \phi\left(\frac{q}{2}\right) + \phi\left(\frac{q}{2}\right) = 2\phi\left(\frac{q}{2}\right)$$

i.e. $\phi(q/2) = 1/2$. But this is not an integer, so no such homomorphism exists.
$\mathbb{R}$ and $\mathbb{C}$ are both uncountable. We have $\mathbb{C} \cong \mathbb{R}^2$, so in deciding whether there is an isomorphism between them we might consider Exercise 3.4, where we showed that $\mathbb{Z} \cong \mathbb{Z}^2$ by constructing a square spiral. However, this does not work here - crucially, $\mathbb{R}$ is dense, while $\mathbb{Z}$ is not, so no such step-wise spiral is possible. So we do not have an isomorphism, but have not disproved that one exists.

Exercise 4.5. Consider $(\mathbb{R}\backslash\{0\}, \cdot)$ and $(\mathbb{C}\backslash\{0\}, \cdot)$. If there exists an isomorphism $\phi : \mathbb{R}\backslash\{0\} \to \mathbb{C}\backslash\{0\}$, it must map 1 to 1. Then,

$$1 = \phi(1) = \phi((-1) \cdot (-1)) = \phi(-1) \cdot \phi(-1)$$

so $\phi(-1) = \pm 1$. But ϕ is injective, so we are forced to have $\phi(-1) = -1$. Then

$$\phi^{-1}(-1) = -1 = \phi^{-1}(i^2) = \phi^{-1}(i)^2$$

so a real non-zero number $\phi^{-1}(i)$ squares to -1. But no such real number exists, and therefore neither does the isomorphism.

Exercise 4.6. If $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}^{>0}, \cdot)$ is an isomorphism, we have $\phi(q + q) = \phi(q)^2$, but this implies that every rational has a square root also in the rationals, which is not true. So no such isomorphism exists.

Exercise 4.7. Define a homomorphism $\phi : G \to G$ by $\phi(g) = g^{-1}$. Then

$$\begin{aligned}\phi(g_1g_2) &= \phi(g_1)\phi(g_2)\\(g_1g_2)^{-1} &= g_1^{-1}g_2^{-1}\\g_2^{-1}g_1^{-1} &= g_1^{-1}g_2^{-1}\end{aligned}$$

for all $g_1, g_2 \in G$. But then is true iff G is Abelian.
Define a homomorphism $\psi : G \to G$ by $\psi(g) = g^2$. Then

$$\begin{aligned}\psi(g_1g_2) &= \psi(g_1)\psi(g_2)\\(g_1g_2)^2 &= g_1^2g_2^2\\g_1g_2g_1g_2 &= g_1^2g_2^2\end{aligned}$$

for all $g_1, g_2 \in G$. But this is also true iff G is Abelian.

Exercise 4.8. For a group G, define maps $\gamma_g : G \to G$ for each $g \in G$ by $\gamma_g(a) = gag^{-1}$. Suppose $\gamma_g(a) = \gamma_g(b)$. Then $gag^{-1} = gbg^{-1}$, so $a = b$, and γ_g is injective. Let $a \in G$. Then $g^{-1}ag \in G$ and $\gamma_g(g^{-1}ag) = a$, so γ_g is also surjective, and hence a bijection. Then consider

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

so γ_g is also a homomorphism, and hence an isomorphism of G to itself, i.e. an automorphism. Specifically, automorphisms defined in this way are called **inner automorphisms**.
Now consider the function $\phi : G \to \text{Aut}(G)$ taking g to γ_g. Then $\phi(gh)$ is the map$\gamma_{gh} : a \mapsto ghah^{-1}h^{-1}$. But

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

so this is a homomorphism.
Suppose ϕ is the trivial homomorphism, i.e. $\phi(g) = \text{id}_G$. That is, $gag^{-1} = a$ for all $a, g \in G$. This can only be true if G is Abelian. On the other hand, if G is Abelian, every γ_g is the identity, so ϕ must be trivial. So ϕ is trivial iff G is Abelian.

Exercise 4.9. Let m and n be positive integers such that $\gcd(m, n) = 1$. Define $\phi : C_{mn} \to C_m \times C_n$ by $\phi([a]_{mn}) = ([a]_m, [a]_n)$.
Suppose $\phi([a]_{mn}) = \phi([b]_{mn})$. Then $[b]_m = [a]_m$ and $[b]_n = [a]_n$, so either b/a or a/b is an integer multiple of both m and n, so either $b/a \mid m$ and $b/a \mid n$ or $a/b \mid m$ and $a/b \mid n$. But since $\gcd(m, n) = 1$, this is only true for the case $b/a = 1 = a/b$, i.e. $b = a$. Hence ϕ is injective.
Consider $\phi([amn]_{mn}) = ([an]_m, [am]_n)$. Since $\gcd(m, n) = 1$, $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$, and $[n]_m$ generates $\mathbb{Z}/m\mathbb{Z}$, by Corollary 2.5. Then relative primeness of m and n secures

surjectivity. Therefore ϕ is a bijection.
Lastly, consider

$$\begin{aligned}\phi([a]_{mn}[b]_{mn}) &= \phi([a+b]_{mn})\\ &= ([a+b]_m, [a+b]_n)\\ &= ([a]_m, [a]_n)([b]_m, [b]_n)\\ &= \phi([a]_{mn})\phi([b]_{mn})\end{aligned}$$

Exercise 4.10. Let $p \neq q$ be odd integers. As a set,

$$\begin{aligned}(\mathbb{Z}/pq\mathbb{Z})^* &= \{[n]_{pq} \in \mathbb{Z}/pq\mathbb{Z} \mid \gcd(n, pq) = 1\}\\ &\cong \mathbb{Z}/pq\mathbb{Z}\backslash\{[0]_{pq}, [p]_{pq}, [q]_{pq}\}\end{aligned}$$

so

$$|(\mathbb{Z}/pq\mathbb{Z})^*| = |\mathbb{Z}/pq\mathbb{Z}| - 3$$

Now, since p and q are primes, $\gcd(p, q) = 1$, so by the previous exercise, $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, and hence $|\mathbb{Z}/pq\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z}||\mathbb{Z}/q\mathbb{Z}| = pq$. Therefore $|(\mathbb{Z}/pq\mathbb{Z})^*| = pq - 3$. So by Exercise 4.3, $(\mathbb{Z}/pq\mathbb{Z})^*$ is cyclic iff it has an element of order $pq - 3$. Suppose $[n]_{pq}$ is this element. Then $[n^{pq-3}]_{pq} = [1]_{pq}$, so $n^{pq-3} = apq + 1$ for some integer a.
???

Exercise 4.11. We assume that $x^d = 1$ has at most d solutions in $(\mathbb{Z}/p\mathbb{Z})^*$, where p is prime. Let g be an element of maximal order. Then by Exercise 1.15, $|h|$ divides $|g|$ for all $h \in (\mathbb{Z}/p\mathbb{Z})^*$. As a set,

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^* &= \{[n]_p \in \mathbb{Z}/p\mathbb{Z} \mid \gcd(n, p) = 1\}\\ &\cong \mathbb{Z}/p\mathbb{Z}\backslash\{[0]_p\}\end{aligned}$$

so $|(\mathbb{Z}/p\mathbb{Z})^*| = |\mathbb{Z}/p\mathbb{Z}| - 1 = p - 1$. Thus $|h|$ divides $p - 1$ for all $h \in (\mathbb{Z}/p\mathbb{Z})^*$. Now, denote by $\psi(d)$ the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d. If $|a| = d$, then by Proposition 1.6,

$$|a^r| = \frac{d}{\gcd(r, d)}$$

so $|a^r| = d$ iff $\gcd(r, d) = 1$. Thus there are $\phi(d)$ elements of the form $|a^r|$ of the same order as $|a|$, where $\phi(d)$ is Euler's ϕ-function. Thus $\phi(d) \mid \psi(d)$. Now, suppose $\psi(d) \neq 0$, and let $a \in (\mathbb{Z}/p\mathbb{Z})^*$ be of order d. All elements of order d must satisfy $x^d = 1$. Now, we are assuming that this has at most d solutions, but we already have d distinct solutions, given by $1, a, a^2, ..., a^{d-1}$. So in fact, $x^d = 1$ has exactly d solutions, which are these ones.

Then we have to find out which of these are really of order d, rather than of order d/n. But recall again that $|a^r| = d$ iff $\gcd(r, d) = 1$, so in fact precisely $\phi(d)$ of these solutions to $x^d = 1$ are of order d. Therefore we have shown that $\psi(d) = \phi(d)$ or 0. Now, recall that $|h|$ divides $p - 1$ for all $h \in (\mathbb{Z}/p\mathbb{Z})^*$. Then

$$|(\mathbb{Z}/p\mathbb{Z})^*| = \sum_{d|(p-1)} \psi(d)$$

and the LHS is $p - 1$. Since $\psi(d) = \phi(d)$ or 0, we also have

$$\sum_{d|(p-1)} \psi(d) \leq \sum_{d|(p-1)} \phi(d)$$

But it is well known that the RHS is $p - 1$, so in fact this must be an equality. Therefore $\psi(d) = \phi(d)$ for all d dividing $p - 1$. In particular, there is an element of order $p - 1$, so $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Exercise 4.12. Consider $[9]_{31} \in (\mathbb{Z}/31\mathbb{Z})^*$. By the previous exercise, this group is cyclic. As a set,

$$(\mathbb{Z}/31\mathbb{Z})^* \cong /31\mathbb{Z}\{[0]_{31}\}$$

so $|(\mathbb{Z}/31\mathbb{Z})^*| = 30$. Then since the group is cyclic, it must contain an element of order 30. Then from Exercise 1.15 the order of any element must divide 30, i.e. be 1, 2, 3, 5, 6, 10, 15, or 30. Clearly the order of $[9]_{31}$ is not 1. By direct calculation we can check that it is in fact 15.
Now consider $x^3 = 9$ in $(\mathbb{Z}/31\mathbb{Z})^*$. Then $x^{45} = 1$. Its order cannot be 45 itself (since this is greater than the order of the group). Instead it must divide 45. But it also has to divide 30. Therefore it is 1, 3, 5 or 15. The elements of order 1 and 3 can be ruled out. If it is order 15, 9^5 would be 1, which is not the case, and therefore we are left looking at elements of order 5, of which there are, as per the previous exercise, $\phi(5) = 4$. We can check manually that none of these work. There is no solution.

Exercise 4.13. Consider the group

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{([a]_2, [b]_2) \mid a, b = 0, 1\}$$

Any automorphism of this group must map the identity to itself, leaving three elements whose images are to be determined. Then clearly as sets, $\mathrm{Aut}_{\mathsf{Set}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. We just need to check that moving to Grp no further restrictions are placed, that is, that each permutation of the three non-zero elements is a homomorphism. We can check a map is a homomorphism just by looking at generators. Here we have two generators, x and y, and the third non-trivial element is xy. Call these g_1, g_2, g_3 respectively. Since $x^2 = y^2 = 1$, we just need to check the action on xy. Let ϕ be a map from the group to itself that is bijective. We have $\phi(g_1g_2) = \phi(g_3)$, and we can write $\phi(g_3) = g_{\sigma(3)}$, where $\sigma \in S_3$ is the permutation of $\{1,2,3\}$ that ϕ applies to $\{g_1, g_2, g_3\}$. Then ϕ is a homomorphism if $g_{\sigma(1)}g_{\sigma(2)} = g_{\sigma(3)}$. Using the two relations already given, and the third, $xyxy = 1$, we see that in fact any two of g_1, g_2, g_3 multiply to give the third. Therefore ϕ is indeed a homomorphism, and $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$.

Exercise 4.14. Consider $C_n = \{e, g, g^2, ..., g^{n-1}\}$, generated by g. An automorphism must map g to g^r for some $0 \leq r < n$, but this g^r must also generate C_n, and hence we must have $\gcd(r, n) = 1$. This is true for exactly $\phi(n)$ maps, by definition of the Euler ϕ, and hence $|\mathrm{Aut}(C_n)| = \phi(n)$.

Exercise 4.15. $(\mathbb{Z}, +)$ has two generators, ± 1, so any automorphism ϕ must map ± 1 to ± 1, injectively. Therefore there are exactly two automorphisms, i.e. $\mathrm{Aut}(\mathbb{Z}, +) \cong \mathbb{Z}_2$. Following on from the previous exercise, $\mathrm{Aut}(C_n)$ is of order $\phi(n)$, so is in one-to-one correspondence with $(\mathbb{Z}/n\mathbb{Z})^*$. Automorphisms of C_n can be specified by the power g^r they map the generator g to, so denote them by this integer, ψ_r. Then the natural correspondence is given by $\psi_r \to [r]_n$. Define f as this bijection. Clearly $\psi_r \circ \psi_s(g) = g^{r+s}$, so $\psi_r \circ \psi_s = \psi_{r+s}$. Then we just have

$$f(\psi_r\psi_s) = f(\psi_{r+s}) = [r+s]_n = [r]_n + [s]_n$$

so this is a homomorphism, and so as groups $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Now, by Exercise 4.11, if $n = p$ is prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Moreover, it is order $p-1$, so it must be isomorphic to C_{p-1} (as a group). Therefore finally we have $\mathrm{Aut}(C_p) \cong C_{p-1}$.

Exercise 4.16. Wilson's theorem states that a positive integer p is prime iff

$$(p-1)! \equiv -1 \mod p$$

$\Rightarrow$ By Exercise 4.11, if p is prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Moreover, it is order $p-1$, so isomorphic to $C_{p-1} = \{e, g, g^2, ..., g^{p-2}\}$. Suppose $h \in C_{p-1}$ is of order 2. Then $h^2 = e$. But we also have $h = g^r$ for some $0 \leq r < p-1$, so $g^{2r} = e$. $|g| = p-1$, so $2r$ divides $p-1$. The only way for this to be so and for $r < p-1$ is to have $2r = p-1$, which is possible for every odd prime. The one other case is $p = 2$, when clearly $(p-1)! \equiv -1 \mod p$, so we continue, assuming $p > 2$. So $2r = p-1$ and there is exactly one element of order 2, $g^{(p-1)/2}$. Then, since $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$, by Proposition 4.8 exactly one element of $(\mathbb{Z}/p\mathbb{Z})^*$ is of order 2. But it is easy to find this element: $(p-1)^2 = p(p-2)+1$, so $[p-1]_p^2 = [1]_p$. Now, recall that from Exercise 1.8 if a group has exactly one element of order 2, the product of all its elements is just that element. So

$$[1]_p[2]_p...[p-1]_p = [(p-1)!]_p = [p-1]_p$$

In other words, $(p-1)! \equiv (p-1) \mod p = -1 \mod p$.
$\Leftarrow$ On the other hand, suppose $(p-1)! \equiv -1 \mod p$, and that d divides p. Then it also divides $(p-1)!$, and hence must divide $np-1$ for some integer n. That is, for some integers m and n, $md = np-1$, so with $m' = -m$, we have $m'd + np = 1$. But by Exercise 2.13 this means $\gcd(d,p) = 1$. Therefore every d which divides p is relatively prime to p, i.e. $d = p$ only, and hence p is prime.
This proves Wilson's theorem.

Exercise 4.17. From Exercise 4.11, if p is prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, and therefore has an element of order $p-1$, which is its generator. Since this is the maximal order for elements of $(\mathbb{Z}/p\mathbb{Z})^*$, which is also an Abelian group, the order of every other element must divide this, by Exercise 1.15. The largest possible order, besides $p-1$ itself, is then $(p-1)/2$, assuming $p > 2$. Therefore if $[a]_p^r$ is not $[1]_p$ for any $1 \leq r \leq (p-1)/2$, its order must be $p-1$, and it is the generator.
Consider $(\mathbb{Z}/5\mathbb{Z})^*$. We have $(p-1)/2 = 2$, and

$$[2]_5^2 = [4]_5$$

so $|[2]_5| > 2$, and hence it is the generator.
Consider $(\mathbb{Z}/7\mathbb{Z})^*$. We have $(p-1)/2 = 3$. $[2^3]_7 = [8]_7 = [1]_7$, so instead try

$$\begin{aligned} [3]_7^2 &= [2]_7 \\ [3]_7^3 &= [6]_7 \end{aligned}$$

so $[3]_7$ is the generator.
Consider $(\mathbb{Z}/11\mathbb{Z})^*$. We have $(p-1)/2 = 5$, and

$$\begin{aligned} [2]_{11}^2 &= [4]_{11} \\ [2]_{11}^3 &= [8]_{11} \\ [2]_{11}^4 &= [5]_{11} \\ [2]_{11}^5 &= [10]_{11} \end{aligned}$$

so $[2]_{11}$ is the generator.
Consider $(\mathbb{Z}/13\mathbb{Z})^*$. We have $(p-1)/2 = 6$, and

$$\begin{aligned} [2]_{13}^2 &= [4]_{13} \\ [2]_{13}^3 &= [8]_{13} \\ [2]_{13}^4 &= [3]_{13} \\ [2]_{13}^5 &= [6]_{13} \\ [2]_{13}^6 &= [12]_{13} \end{aligned}$$

so $[2]_{13}$ is the generator.

Exercise 4.18. Let $\phi : G \to H$ be an isomorphism. Suppose $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$. Then

$$\phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1)$$

Since ϕ is a bijection, it is in particular surjective, so then $h_1h_2 = h_2h_1$ for all $h_1, h_2 \in H$. The converse is obtained in reverse, so G is commutative iff H is.

5 Free Groups

Exercise 5.1. Suppose (j, G) is final in $\mathcal{F}^A$. Then for any group H and function $f : A \to H$, there is a unique homomorphism $\phi : H \to G$ making

$$\begin{tikzcd}
H \arrow[r, "\phi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"] &
\end{tikzcd}$$

commute. Our best guess is to try $G = \{e\}$, since this is final in Grp. Then ϕ is by necessity the trivial homomorphism, so this is indeed final.

Exercise 5.2. Consider the set-function $\varepsilon : A \to \{e\}$ mapping all $a \in A$ to e, and an arbitrary object (j, G) in $\mathcal{F}^A$. Then if a homomorphism $\phi : \{e\} \to G$ makes

$$\begin{tikzcd}
\{e\} \arrow[r, "\phi"] & G \\
A \arrow[u, "\varepsilon"] \arrow[ur, "j"] &
\end{tikzcd}$$

commute, we must have $j(a) = e_G$ for all $a \in A$, since $\phi(\varepsilon(a)) = e_G$ for all $a \in A$. But this is certainly not true for every $j : A \to G$, so no such homomorphism ϕ exists, and $(\varepsilon, \{e\})$ is not initial in $\mathcal{F}^A$.

Exercise 5.3. For any group G and function $f : A \to G$, there is a unique homomorphism making

$$\begin{tikzcd}
F(A) \arrow[r, "\phi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"] &
\end{tikzcd}$$

commute. Suppose $j(a) = j(b)$. Then $\phi(j(a)) = \phi(j(b))$, so $f(a) = f(b)$, and f is injective if f is. But we can choose G to have the same order as A, and then f to be injective, so j is also injective.

Exercise 5.4. So far we have performed elementary reductions by finding the first appearance of $x^{-1}x$ or xx^{-1} starting from the left of a word. For more general procedures, clearly there is no ambiguity if all such pairs are isolated, for instance if $w = xx^{-1}yx^{-1}x$. The only possible problem is if we have overlapping pairs, such as $xx^{-1}x$. But then whether we choose to eliminate the pair xx^{-1} or $x^{-1}x$, we are left with x. Then if we have $xx^{-1}xx^{-1}$, we can consider the first or last three first, and get xx^{-1} either way. In this fashion we see that in fact there is no ambiguity.
Then, on $F(A)$, for all words w, x, y,

$$w \cdot (x \cdot y) = R(wR(xy)) = R(wxy) = R(R(wx)y) = (w \cdot x) \cdot y$$

so the operation on $F(A)$ is associative.

Exercise 5.5. The set $H^{\oplus A} \subset \mathrm{Hom}_{\mathsf{Set}}(A, H)$ is defined by

$$H^{\oplus A} = \{\alpha : A \to H \mid \alpha(a) \neq e_H \text{ for only finitely many } a \in A\}$$

The group structure on $\mathrm{Hom}_{\mathsf{Set}}(A, H)$ is given by $(\alpha + \beta)(a) = \alpha(a) + \beta(a)$ for all a in A. If $\alpha, \beta \in H^{\oplus A}$, $(\alpha + \beta)(a) \neq e_H$ only for finitely many $a \in A$, so indeed $(\alpha + \beta) \in H^{\oplus A}$, so the operation on $\mathrm{Hom}_{\mathsf{Set}}(A, H)$ induces one on $H^{\oplus A}$. Furthermore, it is associative since H is Abelian. The identity is the map e taking a to e_H for all $a \in A$, so clearly is in $H^{\oplus A}$. Then, the inverse of $\alpha \in \mathrm{Hom}_{\mathsf{Set}}(A, H)$ is the map taking a to $-\alpha(a)$ for all $a \in A$, so if $\alpha \in H^{\oplus A}$, then clearly also $\alpha^{-1} \in H^{\oplus A}$. So we have a group structure on $H^{\oplus A}$, making it a subgroup of $\mathrm{Hom}_{\mathsf{Set}}(A, H)$.

Exercise 5.6. Define homomorphisms $f_1, f_2 : \mathbb{Z} \to F(\{x, y\})$ by $f_1(1) = x$ and $f_2(1) = y$. Then, given homomorphisms $g_1, g_2 : \mathbb{Z} \to G$, define a map $\phi : F(\{x, y\}) \to G$ making

$$\begin{tikzcd}
\mathbb{Z} \arrow[dr, "f_1"] \arrow[drr, bend left, "g_1"] & & \\
& F(\{x,y\}) \arrow[r, "\phi"] & G \\
\mathbb{Z} \arrow[ur, "g_2"] \arrow[urr, bend right, "f_2"] & &
\end{tikzcd}$$

commute. Then we must have $\phi(x) = g_1(1)$ and $\phi(y) = g_2(1)$. Since $F(\{x, y\})$ is the free group of $\{x, y\}$, x and y are its generators. Then if we want ϕ to be a homomorphism, defining it on generators defines it completely, so it is uniquely fixed. Therefore $F(\{x, y\})$ satisfies the universal property for the coproduct of $\mathbb{Z}$ with itself in Grp, $F(\{x, y\}) \cong \mathbb{Z} * \mathbb{Z}$.

Exercise 5.7. From the previous exercise we know that $F(\{x_1, x_2\}) \cong \mathbb{Z} * \mathbb{Z}$, and a unique homomorphism $\phi : F(\{x_1, x_2\}) \to G$ makes

$$\begin{tikzcd}
\mathbb{Z} \arrow[dr, "f_1"] \arrow[drr, bend left, "g_1"] & & \\
& F(\{x_1, x_2\}) \arrow[r, "\phi_2"] & G \\
\mathbb{Z} \arrow[ur, "g_2"] \arrow[urr, bend right, "f_2"] & &
\end{tikzcd}$$

commute, where everything is defined as there, except $(x, y) \mapsto (x_1, x_2)$ and $\phi \mapsto \phi_2$. Now, introduce $F(\{x_1, x_2, x_3\})$. It must have $F(\{x_1, x_2\})$ as a subgroup, and hence we have the inclusion ι_2. Also define homomorphisms $f_3 : \mathbb{Z} \to F(\{x_1, x_2, x_3\})$ and $g_3 : \mathbb{Z} \to g_3$, and a map $\phi_3 : F(\{x_1, x_2, x_3\}) \to G$. Then we have the diagram

$$\begin{tikzcd}
F(\{x_1, x_2\}) \arrow[dr, hook, "\iota_2"] \arrow[drr, bend left, "\phi_2"] & & \\
& F(\{x_1, x_2, x_3\}) \arrow[r, "\phi_3"] & G \\
\mathbb{Z} \arrow[ur, "f_3"] \arrow[urr, bend right, "g_3"'] & &
\end{tikzcd}$$

Then if this commutes, $\phi_3(x_1) = \phi_2(x_1)$, $\phi_3(x_2) = \phi_2(x_2)$, and $\phi_3(x_3) = g_3(1)$. If ϕ_3 is a homomorphism, this fixes it completely. Thus $F(\{x_1, x_2, x_3\})$ satisfies the universal property to be the coproduct of $F(\{x_1, x_2\})$ and $\mathbb{Z}$ in Grp, so in fact $F(\{x_1, x_2, x_3\}) \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z}$ (which is well-defined since $*$ is associative). Thus, if we know that $F(\{x_1, ..., x_n\})$ is the coproduct of n factors of $\mathbb{Z}$, we have, for some choice of functions $g_i : \mathbb{Z} \to G$, a unique homomorphism ϕ_n. Defining the function $\phi_{n+1} : F(\{x_1, ..., x_{n+1}) \to G$, we have the diagram

$$\begin{tikzcd}
F(\{x_1,...,x_n\}) \arrow[dr, hook, "\iota_n"] \arrow[drr, bend left, "\phi_n"] & & \\
& F(\{x_1,...,x_{n+1}\}) \arrow[r, "\phi_{n+1}"] & G \\
\mathbb{Z} \arrow[ur, "f_{n+1}"] \arrow[urr, bend right, "g_{n+1}"'] & &
\end{tikzcd}$$

If this commutes, ϕ_{n+1} satisfies $\phi_{n+1}(x_i) = \phi_n(x_i)$ if $i = 1,...,n$, and $\phi_{n+1}(x_{n+1}) = g_{n+1}(1)$. If ϕ_{n+1} is a homomorphism, this fixes it completely. Therefore $F(\{x_1,...,x_{n+1}) \cong F(\{x_1,...,x_n\}) * \mathbb{Z} \cong \mathbb{Z} * ... * \cong \mathbb{Z}$ with $n+1$ factors of $\mathbb{Z}$. We have this for $n = 2$, so inductively, we have it for all n.
We know from Proposition 5.6 that $F^{Ab}(\{x_1,...,x_n\}) \cong \mathbb{Z}^{\oplus n}$, so this tells us that the coproduct in the category Ab is $\oplus$.

Exercise 5.8. Let $A = \{a_i\}$ and $B = \{b_i\}$. Then the $\{a_i\}$ generate $F(A)$, and the $\{b_i\}$ generate $F(B)$. $A \sqcup B = \{a_i\} \sqcup \{b_i\}$, so $F(A \sqcup B)$ is generated by each of both the $\{a_i\}$ and $\{b_i\}$. Then $F(A), F(B) \subset F(A \sqcup B)$, and we can define inclusions $\iota_A : F(A) \hookrightarrow F(A \sqcup B)$ and $\iota_B : F(B) \hookrightarrow F(A \sqcup B)$. Choose functions $f_A : A \to G$ and $f_B : B \to G$. This specifies unique homomorphisms $\phi_A : F(A) \to G$ and $\phi_B : F(B) \to G$ such that

$$\begin{tikzcd}
A \arrow[dr, "j_A"] \arrow[ddrrr, bend left, "f_A"] & & & \\
& F(A) \arrow[dr, hook, "\iota_A"] \arrow[drr, "\phi_A"] & & \\
& & F(A \sqcup B) & G \\
& F(B) \arrow[ur, hook, "\iota_B"] \arrow[urr, "\phi_B"] & & \\
B \arrow[ur, "j_B"] \arrow[uurrr, bend right, "f_B"'] & & &
\end{tikzcd}$$

commutes. Then if we want to define a map $\phi_{A \sqcup B} : F(A \sqcup B) \to G$ such that if we include it in the diagram it still commutes, we must have

$$\begin{aligned}\phi_{A\sqcup B}(\iota_A(a_i)) = \phi_A(a_i)\\ \phi_{A\sqcup B}(\iota_B(b_i)) = \phi_B(b_i)\end{aligned}$$

If $\phi_{A\sqcup B}$ is a homomorphism, this specifies it completely. Thus (ignoring A, B, and the morphisms from them), we see that $F(A \sqcup B)$ satisfies the universal property to be the coproduct of A and B in Grp, $F(A \sqcup B) = F(A) * F(B)$.
If we restrict to Ab, nothing important changes in the construction, but as observed in the previous question, the corproduct is $\oplus$, so $F^{Ab}(A \sqcup B) = F^{Ab}(A) \oplus F^{Ab}(B)$.

Exercise 5.9. Let $G = \mathbb{Z}^{\oplus N} = \mathbb{Z}\oplus \overset{N}{\dots} \oplus\mathbb{Z} = \mathbb{Z}\times \overset{N}{\dots} \times\mathbb{Z}$, since for Abelian groups the (Cartesian) product and coproduct (direct sum) coincide. Then $G \times G = \mathbb{Z}\times \overset{2N}{\dots} \times\mathbb{Z}$. By Exercise 3.4, $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}$, so $G \cong \mathbb{Z}\times \overset{N}{\dots} \times\mathbb{Z} = G$.

Exercise 5.10. Let $F = F^{Ab}(A)$.

(i) Define an equivalence relation $\sim$ on F by setting $f' \sim f$ iff $f - f' = 2g$ for some $g \in F$.
$\Rightarrow$ Suppose A is finite. Label its elements $a_1, ..., a_n$, and regard these as the generators of F. Then a generic element of F is $\prod a_i^{p_i}$. We have

$$\begin{aligned}\left[\prod_{i=1}^{n} a_i^{p_i}\right] &= \left\{\prod_{j=1}^{n} a_j^{p'_j} = \left(\prod_{i=1}^{n} a_i^{p_i}\right)\left(\prod_{k=1}^{n} a_k^{2q_k}\right) \mid q_k \in \mathbb{Z}\right\}\\ &= \left\{\prod_{j=1}^{n} a_j^{p_j+2q_j} \mid q_j \in \mathbb{Z}\right\}\end{aligned}$$

That is, the conjugacy class of an element is the set of elements differing from it by even powers of generators. Then we have classes $[0]$, $[a_i]$, (but $[a_i^2] = [0]$), $[a_ia_j]$, $i \neq j$, and so on. As well as the single class $[0]$, we have exactly $\binom{n}{k}$ classes with representatives being (linear) products of k generators. Thus,

$$|F/\sim| = \sum_{k=0}^{n}\binom{n}{k} = 2^n = 2^{|A|}$$

$\Leftarrow$ On the other hand, suppose $F/\sim$ is finite. Again label the elements of A a_i, but we leave $|A|$ undetermined. We can construct equivalence classes in the same way, and it is easy to see that the only way we can have a finite number of them is if A itself is finite.
Therefore, $F/\sim$ is finite iff A is, and when this is the case, $|F/\sim| = 2^{|A|}$.

(ii) Assume $F^{Ab}(B) \cong F^{Ab}(A)$. An isomorphism between two groups maps generators to generators, so the order of the sets of generators of each is the same. That is, A is finite iff B is, and $A \cong B$.

6 Subgroups

Exercise 6.1. Consider the matrix groups

$$\begin{aligned}
SL(n;\mathbb{R}) &= \{M \in GL(n;\mathbb{R}) \mid \det M = 1\} \\
SL(n;\mathbb{C}) &= \{M \in GL(n;\mathbb{C}) \mid \det M = 1\} \\
O(n) &= \{M \in GL(n;\mathbb{R}) \mid MM^T = I_n\} \\
SO(n) &= \{M \in O(n) \mid \det M = 1\} \\
U(n) &= \{M \in GL(n;\mathbb{C}) \mid MM^\dagger = I_n\} \\
SU(n) &= \{M \in U(n) \mid \det M = 1\}
\end{aligned}$$

Among these, we have the inclusions

$$\begin{aligned}
SL(n;\mathbb{R}) &\hookrightarrow SL(n;\mathbb{C}) \\
O(n) &\hookrightarrow SL(n;\mathbb{R}) \\
SO(n) &\hookrightarrow O(n) \\
U(n) &\hookrightarrow SL(n;\mathbb{C}) \\
SU(n) &\hookrightarrow U(n) \\
O(n) &\hookrightarrow U(n)
\end{aligned}$$

and compositions of these. All of these groups share the same identity, $I_n = \text{diag}(1, ..., 1)$. If a matrix has all real entries, so does its inverse. If it has unit determinant, so does its inverse. If $MM^T = I_n$, $M^{-1} = M^T$, so $M^{-1}(M^{-1})^T = I_n$, and similarly for Hermitian conjugates. Therefore each inclusion is the inclusion of a subgroup.

Exercise 6.2. Consider the set of matrices of the form

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where $a, b, d \in \mathbb{C}$ and $ad \neq 0$. Then $\det M = ad \neq 0$, so this is a subset of $GL(2;\mathbb{C})$. More generally, if $(a_{ij})_{1 \leq i,j \leq n}$ are complex $n \times n$ matrices with $a_{ij} = 0$ for $i > j$, and non-zero on the diagonal, then $\det a$ is the product of the diagonal elements, which is non-zero, and hence $a \in GL(n;\mathbb{C})$.

Exercise 6.3. If $M \in SU(2)$, $M^\dagger M = I$, so $M^{-1} = M^\dagger$. If we write

$$M = \begin{pmatrix} a+bi & c+di \\ e+fi & g+hi \end{pmatrix}$$

then, since also $\det M = 1$, this is

$$\begin{pmatrix} g+hi & -c-di \\ -e-fi & a+bi \end{pmatrix} = \begin{pmatrix} a-bi & e-fi \\ c-di & g-hi \end{pmatrix}$$

So $g = a$, $h = -b$, $e = -c$, $f = d$, and

$$M = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

$\det M = 1$, so also $a^2 + b^2 + c^2 + d^2 = 1$. So $SU(2) \cong S^3 \subset \mathbb{R}^4$.

Exercise 6.4. Let g be an element of some group G, and consider the exponential map $\epsilon_g : \mathbb{Z} \to G$ defined by $\epsilon_g(n) = g^n$. If we define $f : \mathbb{Z} \to \operatorname{Im} \epsilon_g$ by $f = \epsilon_g$, f is by definition surjective, and g generates $\operatorname{Im} \epsilon_g$. It maps generator to generator, so is a homomorphism. If G is not cyclic, f is also injective, and so an isomorphism. Then $\operatorname{Im} \epsilon_g$ is cylic.

Exercise 6.5. Let G be Abelian and n a positive integer. Define $H = \{g^n \mid g \in G\}$. Then $H \subseteq G$ as sets. We have $e_G = e_G^n$, so $e_G \in H$, and H is non-empty. Then consider $g^n, h^n \in H$. $g^n(h^n)^{-1} = g^n h^{-n} = (gh^{-1})^n$, since G is Abelian. Then $gh^{-1} \in G$ so $(gh^{-1})^n \in H$, and H is a subgroup. If G is not Abelian, $g^n h^{-n}$ is not necessarily g'^m for any $g \in G$ or $m \in \mathbb{Z}^{>0}$.

Exercise 6.6.

(i) Let H, H' be subgroups of G, and consider $H \cup H'$. Let $h \in H$ and $h' \in H'$. Then $H \cup H'$ is a subgroup if $hh'^{-1} \in H \cup H'$, since the case where h, h' are both in either H or H' is trivial. So $hh'^{-1} \in H$ and/or $hh'^{-1} \in H'$. But then either $H' \subseteq H$ or $H \subseteq H'$.

(ii) Let $H_0 \subseteq H_1 \subseteq ...$ be subgroups of G, and consider $H = \bigcup_i H_i$. Let $h, h' \in H$, so $h \in H_i$, $h' \in H_j$ for some i, j. Without loss of generality, suppose $i \leq j$. Then $H_i \subseteq H_j$, so $h, h' \in H_j$, and hence $hh'^{-1} \in H_j \subset H$. So H is a subgroup of G.

Exercise 6.7.

(i) Inner automorphisms of a group G are homomorphisms $\gamma_g : a \mapsto gag^{-1}$. The set of inner automorphisms is $\text{Inn}(G) \subseteq \text{Aut}(G)$. Let $\gamma_g, \gamma_h \in \text{Inn}(G)$. Then $\gamma_g \circ \gamma_h^{-1} = \gamma_g(h^{-1}ah) = gh^{-1}ahg^{-1} = \gamma_{gh^{-1}}(a) \in \text{Inn}(G)$, so $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.

(ii) Suppose $\text{Inn}(G)$ is cyclic. Then there is some $a \in G$ such that, for each $g \in G$ there exists an integer n making $\gamma_g = \gamma_a^n$. In particular, $\gamma_g(a) = \gamma_a^n(a)$, which is $gag^{-1} = a$, so a commutes with each $g \in G$. Then γ_a is the identity on G, but every other inner automorphism is $\gamma_g = \gamma_a^n$ for some n, and hence they are all the identity, and $\text{Inn}(G)$ is trivial.
Suppose $\text{Inn}(G)$ is trivial. Then $\gamma_g(a) = a$ for all $a, g \in G$, so G is Abelian.
Suppose G is Abelian. Then $\gamma_g(a) = a$ for all $a, g \in G$, so in particular, if we choose some fixed a, $\gamma_g = \gamma_a$ for all g, which confirms the statement that there exists some n such that $\gamma_g = \gamma_a^n$, so $\text{Inn}(G)$ is cyclic.
Therefore, $\text{Inn}(G)$ is cylic iff $\text{Inn}(G)$ is trivial iff G is Abelian.

Exercise 6.8. A group G is finitely generated iff there exists a surjective homomorphism $F(\{1, ..., n\}) \to G$ for some n. If G is Abelian, $F(\{1, ..., n\})$ must be, so in fact we have $F^{Ab}(\{1, ..., n\}) \cong \mathbb{Z}^{\oplus n}$, and therefore we want a surjective homomorphism $\mathbb{Z} \oplus ... \oplus \mathbb{Z} \to G$.

Exercise 6.9.

(i) Let $A \subseteq \mathbb{Q}$ as a set. If A is finite, we can write $A = \{p_i/q_i \mid i = 1, ..., n\}$. Then

$$\langle A \rangle = \left\{ \frac{p}{q} = \sum_{i=1}^{n} m_i \frac{p_i}{q_i} \mid m_i \in \mathbb{Z} \right\}$$

Let $r = 1/(q_1...q_n) \in \mathbb{Q}$. Then

$$\langle r \rangle = \left\{ \frac{s}{q_1...q_n} \mid s \in \mathbb{Z} \right\}$$

and hence $\langle A \rangle \subseteq \langle r \rangle$. But clearly $\langle r \rangle$ is cyclic, so by Proposition 6.9, so must $\langle A \rangle$ be.

(ii) Suppose $\mathbb{Q}$ is finitely generated, and let these generators be p_i/q_i, $i = 1, ..., n$. Then every $r \in \mathbb{Q}$ is a sum $\sum_{i=1}^{n} m_i p_i/q_i$ where the $m_i \in \mathbb{Z}$. But this can be reexpressed as $m'/q_1...q_n$ for some $m' \in \mathbb{Z}$. Let p be a prime not dividing $q_1...q_n$, and consider $r = 1/p$. Then $1/p = m'/q_1...q_n$, but then m' is not an integer. Therefore by contradiction, $\mathbb{Q}$ is not finitely generated.

Exercise 6.10. Consider

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Let $H = \langle s, t \rangle$. Then

$$t^{-q} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$$

and

$$s^3 t^q s = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$$

so these matrices are in H. Now, let $c, d \neq 0$, and

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2; \mathbb{Z})$$

Consider

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix}$$

If $c \mid d$, let $q = d/c$, and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -d/c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -ad/c + b \\ c & 0 \end{pmatrix}$$

If $d \mid c$, let $q = c/d$, and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -c/d & 1 \end{pmatrix} = \begin{pmatrix} a + bc/d & b \\ 0 & d \end{pmatrix}$$

I'm not totally sure of how to generalise to all c, d, and I do not feel an overwhelming desire to work it out. Once we have done this, we know how to use elements of H to set either c or d to zero. The result is a product of m, s and t. But all of these have unit determinant, so so do their products. Thus the resulting matrix is in $SL(2; \mathbb{Z})$, and therefore this group is finitely generated by $\{s, t\}$.

Exercise 6.11. Every finitely generated Abelian group is a coproduct of cyclic groups in Ab. Consider instead Grp, and S_3. Let G and H be cyclic groups, with generators g and h, respectively. Let $\iota_G : G \to S_3$ and $\iota_H : H \to S_3$ be homomorphisms. Without loss of generality, let $\iota_G(g) = x$ and $\iota_H(h) = y$, where $|x| = 2$ and $|y| = 3$. Introduce a group F and homomorphisms $f_G : G \to F$ and $f_H : H \to F$. Then let $\phi : S_3 \to F$ be such that

$$\begin{tikzcd}
G \arrow[dr, "\iota_G"] \arrow[drr, bend left, "f_G"] & & \\
& S_3 \arrow[r, "\phi"] & F \\
H \arrow[ur, "\iota_H"] \arrow[urr, bend right, "f_H"'] & &
\end{tikzcd}$$

commutes. Then $\phi(x) = f_G(g)$ and $\phi(y) = f_H(y)$. If ϕ is a homomorphism, this defines it completely. Then consider

$$\phi(xyx^{-1}y^{-1}) = f_G(g)f_H(h)f_G(g)^{-1}f_H(h)^{-1}$$

Choose F to be Abelian. Then the RHS is e_F, but $xyx^{-1}y^{-1} \neq e_{S_3}$, so ϕ is not a homomorphism. Therefore, by contradiction, such a ϕ does not exist for any group F, and hence S_3 is not a coproduct of cyclic groups. It follows that not every finitely generated group is a coproduct in Grp.

Exercise 6.12. Consider positive integers m and n, and the subgroup $\langle m, n\rangle$ of $\mathbb{Z}$ they generate.

$$\langle m, n\rangle = \{am + bc \mid a, b \in \mathbb{Z}\}$$

By Proposition 6.9, $\langle m, n\rangle = d\mathbb{Z}$ for some d, namely, the smallest positive $d = am + bc$ for integers a and b. If m divides n, this is m, and $\langle m, n\rangle = \langle m\rangle = m\mathbb{Z}$, and similarly if n divides m. In both cases, $d =$gcd(m, n). Otherwise, let $c =$gcd(m, n), so $m = cp$ and $n = cq$ for primes p, q. Then $d = c(ap + bq)$. To get the smallest positive value of this, notice that since $\gcd(p, q) = 1$, there exist integers a' and b' such that $a'p + b'q = 1$. So making this choice, we see that $d = c =$gcd(m, n). Therefore in general,

$$\langle m, n\rangle = \gcd(m, n)\mathbb{Z}$$

Exercise 6.13 (Omitted)**.**

Exercise 6.14. Consider the sum

$$\sum_{m|n} \phi(m)$$

This may be regarded as the sum over subgroups of C_n, each of which is isomorphic to some C_m with $m \mid n$. $\phi(m)$ is the number of generator of C_m, and hence the number of generators of the subgroup of C_n which is isomorphic to C_m. So

$$\sum_{m|n} \phi(m) = \sum_{\text{subgroups of } C_n} \# \text{ generators}$$

But each element of C_n generates a subgroup, so the RHS must be n itself:

$$\sum_{m|n} \phi(m) = n$$

Exercise 6.15. Let $\phi : G \to G'$ be a homomorphism, and ψ a left-inverse of ϕ. Then let $\alpha, \beta : H \to G$ be homomorphisms. Then if $\phi \circ \alpha = \phi \circ \beta$, composing on the left with ψ gives us $\alpha = \beta$. Conversely, obviously if $\alpha = \beta$, $\phi \circ \alpha = \phi \circ \beta$. So ϕ is a monomorphism.

Exercise 6.16. Let $\phi : \mathbb{Z}/3\mathbb{Z} \to S_3$ be a homomorphism, defined by $\phi([1]_3) = y$, where $|y| = 3$. If ψ is a left-inverse of ϕ, it must be defined by $\psi(y) = [1]_3$ and $\psi(x) = [n]_3$ for some n which we can choose to be less than 3. Then consider

$$\begin{aligned} \psi(xy) &= \psi(x)\psi(y) = [n+1]_3 \\ \psi(yx^{-1}) &= \psi(y)\psi(x)^{-1} = [1-n]_3 \end{aligned}$$

But these are equal, so $[n+1]_3 = [1-n]_3$, or $[2n]_3 = [0]_3$. But no such $n < 3$ exists. Therefore ϕ does not have a left-inverse.

7 Quotient Groups

Exercise 7.1. The subgroups of S_3, with the generators x and y, where $|x| = 2$ and $|y| = 3$, are

- $\{e\}$. Trivially normal.
- $\{e, x\}$. We have

  $$\begin{aligned} xxx^{-1} &= x \in \{e, x\} \\ yxy^{-1} &= xy^2y^{-1} = xy \notin \{e, x\} \end{aligned}$$

  so this is not normal.
- $\{e, y, y^2\}$. We have

  $$\begin{aligned} xyx^{-1} &= xyx = xxy^2 = y^2 \in \{e, y, y^2\} \\ xy^2x^[-1 &= yxx^{-1} = y \in \{e, y, y^2\} \\ yyy^{-1} &= y \in \{e, y, y^2\} \\ yy^2y^{-1} &= y^2 \in \{e, y, y^2\} \end{aligned}$$

  and it is sufficient to check on generators, so this is normal.

Exercise 7.2. Let $\phi : G \to G'$ be a homomorphism. If $g \in \operatorname{Im}\phi$ and $g' \in G'$ are arbitrary, $\operatorname{Im}\phi$ is a normal subgroup of G' if $g'gg'^{-1} \in \operatorname{Im}\phi$. This is not necessarily true (but of course it is if G' is Abelian).

Exercise 7.3. $N \subset G$ is normal if $gng^{-1} \in N$ for all $g \in G$, $n \in N$. Then

(i) $gNg^{-1} = \{gng^{-1} \mid n \in N\} \subseteq N$

(ii) By multiplying on the left by g^{-1} and on the right by g, we also have $N \subseteq g^{-1}Ng$, so in fact $gNg^{-1} = N$

(iii) Then also $gN = Ng$

Exercise 7.4. In Exercise 5.10, we considered the free Abelian group $F = F^{Ab}(A)$ and the equivalence relation $f' \sim f$ iff $f - f' = 2g$ for some $g \in F$. Suppose $f' \sim f$. Then

(i) $(f + g') - (f' + g') = 2g$ so $f + g' \sim f' + g'$

(ii) Then also $g' + f \sim g' + f'$ by commutativity

so $\sim$ is compatible with F. Then, we have $H = \{f \mid f \sim 0\} = \{2g \mid g \in F\}$, so

$$F/\sim = \{f + H \mid f \in F\} = \{f + 2g \mid f, g \in F\}$$

What is this group?

Exercise 7.5. Let $A, A' \in SL(2;\mathbb{Z})$ and define an equivalence relation by $A \sim A'$ iff $A = \pm A'$. Then if $A \sim A'$, and $M \in SL(2;\mathbb{Z})$, $MA = \pm MA'$, so $MA \sim MA'$, and $AM = \pm A'M$, so $AM \sim A'M$. Therefore $\sim$ is compatible with $SL(2;\mathbb{Z})$, and we can define the quotient group $PSL(2;\mathbb{Z}) = SL(2;\mathbb{Z})/\sim$, called the **modular group**. Now, as per Exercise 6.10, $SL(2,\mathbb{Z})$ is generated by

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Let

$$t' = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

Then note that

$$t's = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

which is t in $PSL(2;\mathbb{Z})$. Therefore any element of $PSL(2;\mathbb{Z})$ can be written as a product of s and t'. To show that both are necessary to write an arbitrary element, and hence that they are the generators of $PSL(2;\mathbb{Z})$, we note that while $|s| = 2$ and $|t'| = 3$, $|st'| = \infty$.

Exercise 7.6. Let n be a positive integer, and define a relation on a group G by $a \sim b$ iff there exists some $g \in G$ such that $ab^{-1} = g^n$. Then

(i) $aa^{-1} = e^n$ for any n, so $a \sim a$.
If $a \sim b$, for some g $ab^{-1} = g^n$. Then $ba^{-1} = (ab^{-1})^{-1} = g^{-n}$, and indeed $g^{-1} \in G$, so $b \sim a$.
If $a \sim b$ and $b \sim c$, for some $g, g' \in G$ we have $ab^{-1} = g^n$ and $bc^{-1} = g'^n$, so $ac^{-1} = g^n g'^n$. However, $g^n g'^n \neq g''^n$ in general, so $\sim$ is not in general an equivalence relation.

(ii) However, if G is Abelian, $g^n g'^n = (gg')^n$, and $gg' \in G$, so $a \sim c$ and $\sim$ is an equivalence relation. Corresponding to $\sim$ we have

$$\begin{aligned} H &= \{h \sim e \mid h \in G\} \\ &= \{h \mid \exists g \in G, h = g^n\} \\ &= \{g^n \mid g \in G\} \end{aligned}$$

Exercise 7.7. Let G be a group and define

$$H = \{h \in G \mid |h| = n\}$$

Consider

$$(ghg^{-1})^n = ghg^{-1}ghg^{-1}...ghg^{-1} = gh^n g^{-1} = geg^{-1} = e$$

so $|ghg^{-1}|$ divides n. Suppose $|ghg^{-1}| = m < n$. Then $gh^m g^{-1} = e$, so $gh^m = g$, so $h^m = e$. But this is not true of any $m < n$, so in fact $|ghg^{-1}| = n$. Thus H is normal.

Exercise 7.8.
Proposition. If H is any subgroup of a group G, the relation $\sim_L$ defined by

$$a \sim_L b \Leftrightarrow a^{-1}b \in H$$

is an equivalence relation satisfying

$$a \sim_L b \Rightarrow ga \sim gb$$

Proof. $e_G \in H$ for any subgroup H, so $a \sim_L a$.
If $a^{-1}b \in H$, $(a^{-1}b)^{-1} = b^{-1}a \in H$, so $a \sim_L b \Rightarrow b \sim_L a$.
If $a^{-1}b, b^{-1}c \in H$, $a^{-1}bb^{-1}c = a^{-1}c \in H$, so $a \sim_L b$ and $b \sim_L c$ imply $a \sim_L c$.
Therefore $\sim_L$ is an equivalence relation. Furthermore, if $a^{-1}b \in H$, $a^{-1}b = a^{-1}g^{-1}gb \in H$, so $ga \sim gb$. □

Exercise 7.9.

Proposition. Let $\sim$ be an equivalence relation on a group G satisfying $a \sim b \Rightarrow ag \sim bg$. Then

(i) The equivalence class of e_G is a subgroup H of G

(ii) $a \sim b \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$

Proof.

(i) $H \neq \emptyset$, so let $a, b \in H$. Then $a \sim e_G$ so $e_G \sim a^{-1}$ and $b \sim a^{-1}b$, so $a^{-1}b \sim e_G$ and hence $a^{-1}b \in H$.

(ii) Suppose $a \sim b$. Then $ab^{-1} \sim e_G$ so $ab^{-1} \in H$.
Suppose $ab^{-1} \in H$. Then $Hab^{-1} \subseteq H$, so $Ha \subseteq Hb$. But by symmetry of $\sim$ we also have $Hb \subseteq H_a$, so $Ha = Hb$.
Suppose $Ha = Hb$. Then $a = e_G a \in Ha = Hb$, so $ab^{-1} \in H$, so $e_G \sim ab^{-1}$. Therefore $a \sim b$.

□

Proposition. If H is any subgroup of a group G, the relation $\sim_R$ defined by

$$a \sim_R b \Leftrightarrow ab^{-1}H$$

is an equivalence relation satisfying

$$a \sim_R b \Rightarrow ab^{-1} \in H$$

Proof. $e_G \in H$, so $a \sim_R a$.
If $ab^{-1} \in H$, $ba^{-1} \in H$, so $a \sim_R b \Rightarrow b \sim a_R$.
If $ab^{-1}, bc^{-1} \in H$, $ac^{-1} = ab^{-1}bc^{-1} \in H$, so $a \sim_R b$ and $b \sim_R c$ imply $a \sim_R c$.
Therefore $\sim_R$ is an equivalence relation. Furthermore, if $ab^{-1} \in H$, $agg^{-1}b^{-1} \in H$, so $ag \sim_R bg$. □

Exercise 7.10. Let H be a subgroup of G.
$\Rightarrow$ Suppose H is normal. Consider $\gamma_g \in \mathrm{Inn}(G)$, defined by $\gamma_g(a) = gag^{-1}$. Then if $h \in H$, $\gamma_g(h) = ghg^{-1} \in H$, so $\gamma_g(H) \subseteq H$.
$\Leftarrow$ Suppose $\gamma_g(H) \subseteq H$ for all $g \in G$. But

$$\gamma_g(H) = \{ghg^{-1} \mid h \in H\} = ghg^{-1}$$

and $gHg^{-1} \subseteq H$ means H is normal.
Therefore H is normal iff $\gamma(H) \subseteq H$ for all $\gamma \in \mathrm{Inn}(G)$.
Then we have a map $\phi : \mathrm{Inn}(G) \to \mathrm{Aut}(H)$ given by $(\phi(\gamma_g))(h) = ghg^{-1}$. Then

$$\begin{aligned}(\phi(\gamma_g\gamma_{g'}))(h) &= (\phi(\gamma_{gg'}))(h)\\ &= gg'hg'^{-1}g^{-1}\\ &= (\phi(\gamma_g))(g'hg'^{-1})\\ &= (\phi(\gamma_g)\phi(\gamma_{g'}))(h)\end{aligned}$$

so this is a homomorphism.

Exercise 7.11. Given a group G, define the **commutator subgroup** of G by

$$[G,G] = \{aba^{-1}b^{-1} \mid a,b \in G\}$$

Let $c \in [G,G]$. Then $gcg^{-1}c^{-1} \in [G,G]$ and $c^{-1} \in [G,G]$, so also $gcg^{-1} \in [G,G]$. So $[G,G]$ is a normal subgroup. Now, consider $ghg^{-1}h^{-1}[G,G]$. The $ghg^{-1}h^{-1}$ factor is itself in $[G,G]$, so this is just $[G,G]$ itself by closure of subgroups. Therefore

$$(gh[G,G])(g^{-1}h^{-1}[G,G]) = e[G,G]$$

so

$$gh[G,G] = hg[G,G]$$

and hence $G/[G,G]$ is Abelian.

Exercise 7.12. Let $F = F(A)$ be a free group, and $f : A \to G$ be a set-function, where G is a group. Then by the universal property of free groups, there is a unique homomorphism ϕ making

$$\begin{tikzcd} F(A) \arrow[r, "\phi"] & G \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$$

commute. Now, Theorem 7.12 tells us that given a group $F = F(A)$ and homomorphism $\phi : F \to G$, there is a unique homomorphism $\tilde{\phi}$ making

$$\begin{tikzcd} F \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & G \\ & F/[F,F] \arrow[ur, "\tilde{\phi}"'] & \end{tikzcd}$$

commute, as long as $[F, F] \subset \ker \phi$. Suppose G is Abelian. Then indeed

$$\phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = e_G$$

Now, we can combine these two diagrams to create

$$\begin{tikzcd}
& A \arrow[dl, "j"'] \arrow[dr, "f"] & \\
F \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & G \\
& F/[F,F] \arrow[ur, "\tilde{\phi}"'] &
\end{tikzcd}$$

where $\tilde{\phi}$ is the unique homomorphism making this commute, for given f. Then in particular, $\tilde{\phi}$ is the unique homomorphism making

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\pi\circ j"] & G \\
F/[F,F] \arrow[ur, "\tilde{\phi}"] &
\end{tikzcd}$$

commute given f, for any Abelian group G. That is, $F/[F, F]$ satisfies the universal property for free groups in Ab, so

$$F/[F, F] \cong F^{Ab}(A)$$

Exercise 7.13. Let A and B be sets, $F(A)$ and $F(B)$ be free groups, and suppose $F(A) \cong F(B)$. In Exercise 5.10 we observed that if $F^{Ab}(A) \cong F^{Ab}(B)$ then A is finite iff B is, and $A \cong B$. Using the previous exercise, we can construct the diagram

$$\begin{tikzcd}
& A \arrow[dl, "j_A"'] \arrow[dr, "f_A"] & & B \arrow[dl, "f_B"'] \arrow[dr, "j_B"] & \\
F(A) \arrow[rr, "\phi_A"] \arrow[dr, "\pi_A"'] & & G & & F(B) \arrow[ll, "\phi_B"] \arrow[dl, "\pi_B"] \\
& F^{Ab}(A) \arrow[ur, "\tilde{\phi}_A"'] & & F^{Ab}(B) \arrow[ul, "\tilde{\phi}_B"] &
\end{tikzcd}$$

If $F(A) \cong F(B)$, they satisfy the same universal property, so can be swapped (along with the morphisms attached to them) at will. But this implies we can do the same for $F^{Ab}(A)$ and $F^{Ab}(B)$. Therefore $F^{Ab}(A) \cong F^{Ab}(B)$, and we can import the results of Exercise 5.10: A is finite iff B is, and $A \cong B$.

8 Canonical Decomposition and Lagrange's Theorem

Exercise 8.1. $\mathbb{Z}/2\mathbb{Z}$ is a subgroup of both $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We have

$$\frac{\mathbb{Z}/4\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$$

and

$$\frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$$

However,

$$\mathbb{Z}4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Therefore it is not generally true that $G/H \cong G'/H$ implies $G \cong G'$.

Exercise 8.2. Let $H \subset G$ be a subgroup of index 2. If $g \in H$, obviously $gH = H = Hg$. If $g \notin H$, since cosets partition G, and there are exactly two cosets, we must have $gH \in G\backslash H$. Similarly $Hg = G\backslash H$, so $gH = Hg$. Therefore G is normal.

Exercise 8.3. Let G be finite, and $(A \mid \mathcal{R})$ a presentation of G. $A \subseteq G$ as sets, so A is also finite (more exactly, we could make A bigger than G, compensating with extra relations, but we can always choose A smaller than or equal to G). Then, $F(A)$ is finitely generated by definition, so any subgroup of it is also. But $R \subseteq F(A)$, and $\mathcal{R}$ generates R, so $\mathcal{R}$ is finite (again, this continues to assume that we have chosen to make A finite, which is always possible). Thus G is finitely presented.

Exercise 8.4. Consider $(a, b \mid a^2, b^2, (ab)^n)$. Write $a = x$, $b = xy$. Then we can regard the group as being generated. by x and y, subject to

$$\begin{gathered} x^2 = e \\ xyxy = e \Rightarrow xy = y^{-1}x^{-1} = y^{-1}x \\ (x^2y)^n = e \Rightarrow y^n = e \end{gathered}$$

But this is just D_{2n}.

Exercise 8.5. Let $a, b \in G$, $|a| = |b| = 2$, and $|ab| = n$, where n is finite and ≥ 3. Then $a^2 = e$, $b^2 = e$, and $(ab)^n = e$, which is just D_{2n}, i.e. $G \supset \langle a, b \rangle \cong D_{2n}$.

Exercise 8.6. Suppose the Cayley graph of G generated by A is a tree. Then for any $g_1, g_2 \in G$, there is at most one $a \in A$ such that $g_2 = g_1 a$, so there are no closed loops. But a relation $a_{i_1}^{j_1}...a_{i_n}^{j_n}$ implies a closed loop $e \to a_{i_1} \to a_{i_1}^{2} \to ... \to a_{i_1}^{j_1} \to ... \to a_{i_n}^{j_{n-1}} \to e$. So there can be no relations, and G is freely generated by A. It is easy to see how this also goes in the opposite direction. Therefore G is freely generated by A iff the associated Cayley graph is a tree.

Exercise 8.7. Let G and G' be two groups, with presentations $(A \mid \mathcal{R})$ and $(A' \mid \mathcal{R}')$ respectively. Denote their coproduct $G * G'$. Then, for any group H, and homomorphisms $f : G \to H$ and $f' : G' \to H$, there is a unique homomorphism $\sigma : G * G' \to H$ making

$$\begin{tikzcd}
G \arrow[dr, hook, "\iota"] \arrow[drr, bend left, "f"] & & \\
& G * G' \arrow[r, "\sigma"] & H \\
G' \arrow[ur, hook, "\iota'"] \arrow[urr, bend right, "f'"'] & &
\end{tikzcd}$$

commute. Now, claim that $G * G'$ has the presentation $(A \cup A' \mid \mathcal{R} \cup \mathcal{R}')$. Then we have the natural inclusions

$$\begin{aligned}
\iota(a) &= a \quad \forall a \in A \\
\iota'(a') &= a' \quad \forall a' \in A'
\end{aligned}$$

Then require, for all $a \in A$, that

$$\sigma \circ \iota(a) = \sigma(a) = f(a)$$

and for all $a' \in A'$, that

$$\sigma \circ \iota'(a') = \sigma(a') = f'(a')$$

Since $A \cup A'$ generates $G * G'$, this defines σ completely and uniquely. Relations can be regarded as conditions on all homomorphisms out of a group - the fact that here we have exactly $\mathcal{R} \cup \mathcal{R}'$, where $\mathcal{R} \cap \mathcal{R}' = \emptyset$, means that σ is well-defined given f and f'.

Exercise 8.8. Consider $SL(n;\mathbb{R}) \subset GL(n;\mathbb{R})$. Let $A \in SL(n;\mathbb{R})$ and $M \in GL(n;\mathbb{R})$. Then

$$\begin{aligned}
\det\bigl(MAM^{-1}\bigr) &= \det M \det A \det M^{-1} \\
&= \det A \\
&= 1
\end{aligned}$$

so $MAM^{-1} \in SL(n;\mathbb{R})$. Therefore $SL(n;\mathbb{R})$ is normal in $GL(n;\mathbb{R})$.
Consider the homomorphism $\det : GL(n;\mathbb{R}) \to \mathbb{R}\backslash\{0\}$, the multiplicative group. This is surjective, and $\ker\det = SL(n;\mathbb{R})$. Therefore, by the first isomorphism theorem,

$$GL(n;\mathbb{R})/SL(n;\mathbb{R}) \cong \mathbb{R}$$

Exercise 8.9. Any $M \in SO(3)$ has the form

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

while any $A \in SU(2)$ has the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

Then clearly we can surject from $SU(2)$ onto $SO(3)$. In the kernel,

$$a^2+b^2-c^2-d^2 = a^2-b^2+c^2-d^2 = a^2-b^2-c^2+d^2 = 1$$
$$ad+bc = bd-ac = bc-ad = ab+cd = ac+bd = cd-ab = 0$$

That is, $a = \pm 1$ and $b = c = d = 0$. Then the kernel of the surjection is $\{\pm I_2\}$, and hence

$$SO(3) \cong SU(2)/\{\pm I_2\}$$

$SU(2)$ is simply connected, so homotopically trivial. So the fundamental group of $SO(3)$ is $\{\pm I_2\} \cong C_2$.

Exercise 8.10. Consider $\mathbb{Z}\times\mathbb{Z} \subset \mathbb{R}\times\mathbb{R}$. From Example 8.3, we have

$$\frac{\mathbb{R}\times\mathbb{R}}{\mathbb{Z}\times\mathbb{Z}} \cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}}$$

But as in Example 8.7, $\mathbb{R}/\mathbb{Z} \cong S^1$, so we have

$$\frac{\mathbb{R}\times\mathbb{R}}{\mathbb{Z}\times\mathbb{Z}} \cong S^1 \times S^1$$

which is just the torus.

Exercise 8.11. Let $H \subseteq N \subseteq G$ be subgroups.
$\Rightarrow$ Let N be normal in G. Then $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Then, $N/H = \{nH \mid n \in N\}$ and $G/H = \{gH \mid g \in G\}$. Consider $(gH)(nH)(gH)^{-1} = ((gng^{-1})H)$. But this is in N/H, so N/H is normal in G/H.
$\Leftarrow$ This also works in the opposite direction.
Therefore, N is normal in G iff N/H is normal in G/H.

Exercise 8.12. $HK = \{hk \in G \mid h \in H, k \in K\}$. Let H, K be subgroups of G, and $hk, h'k' \in HK$. Then

$$(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} = hk''h'^{-1}$$

where $k'' \in K$. Then

$$hk'' = hk''h'^{-1}k''^{-1}k'' = hk'''k''$$

since H is normal, so

$$(hk)(h'k')^{-1} = hk'''' \in HK$$

Therefore HK is a subgroup of G.

Exercise 8.13. Let G be finite and Abelian, $|G|$ be odd and $g \in G$. Consider the map $\phi : G \to G$ defined by $\phi(g) = g^2$. This is a homomorphism since G is Abelian. We want to show that it is surjective. But since it is an endomorphism, this is equivalent to it being injective. So suppose $g^2 = h^2$. $|G| = n$ is odd, so $n+1$ is even, and we can write $n+1 = 2k$ for some integer k. Then $g = g^{n+1} = g^{2k}$, and similarly $h = h^{2k}$. But $g^2 = h^2$ implies $g^{2k} = h^{2k}$, and hence $g = h$. Therefore ϕ is injective, so surjective. Every element of G is a square.

Exercise 8.14. Let $|G| = n$ and define $\phi : G \to G$ by $\phi(g) = g^k$, where $\gcd(n, k) = 1$. We have $g = g^{n+1}$ and $h = h^{n+1}$. Since $\gcd(n, k) = 1$, we can choose integers a and b such that $an + bk = 1$, i.e. $bk = 1 - an$. Then suppose $g^k = h^k$. We have

$$\begin{aligned} g^k &= h^k \\ g^{bk} &= h^{bk} \\ g^{1-an} &= h^{1-an} \\ g &= h \end{aligned}$$

So ϕ is injective, but since it is an endomorphism, it is also surjective. Therefore every element of G is a k^{th} power for every k relatively prime to $n = |G|$.

Exercise 8.15. Let a, n be positive integers, and $a > 1$. Consider $(\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$. This has order $\phi(a^n - 1)$. Clearly $[a]_{a^n-1} \in (\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$, so we have the subgroup

$$\langle [a]_{a^n-1} \rangle \subseteq (\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$$

and by Lagrange's theorem $| \langle [a]_{a^n-1} \rangle |$ divides $|(\mathbb{Z}/(a^n - 1)\mathbb{Z})^*|$. That is, $|[a]_{a^n-1}|$ divides $\phi(a^n - 1)$. Now,

$$[a]^n_{a^n-1} = [a^n]_{a^n-1} = [a]_{a^n-1}$$

and indeed clearly $|[a]_{a^n-1}| = n$, since n is the first power for which $a^n \geq a^n - 1$. So n divides $\phi(a^n - 1)$.

Exercise 8.16. Fermat's little theorem states that if p is prime, $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ so $|[a]| = p-1$ and hence $a^p = a \mod p$. Now, consider any integer n. If $\gcd(a, n) = 1$, $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, and we can proceed as in the special case that n is prime. We have $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$, and $|[a]_n| \leq \phi(n)$ divides $\phi(n)$ by Lagrange's theorem. Write $|[a]_n| = d = \phi(n)/k$. Then

$$[a]_n^{\phi(n)} = [1]_n$$

so $a^{\phi(n)} = 1 \mod n$.

Exercise 8.17. Let G be finite and Abelian, and p a prime divisor of $|G|$. Let g be any non-trivial element. We have the subgroup $\langle g \rangle = \{e, g, g^2, ...\}$, which is cyclic, i.e. $\langle g \rangle \cong Z/d\mathbb{Z}$, where $d = | \langle g \rangle | = |g|$. If q is prime, $\gcd(p, q) = 1$, so $ad + bq = 1$ for some integers a and b. Then

$$g^{bq} = g^{-ad} = e$$

so $|g^b| = q$, and $g^b \in G$ is an element of prime order q. If $q = p$, then we have shown that G contains an element of prime order p. Suppose $p \neq q$, and now consider $G/\langle g \rangle$. This can be regarded as G with all factors of g deleted, i.e. as G with the relation $g = e$. Now, by Lagrange's theorem

$$|G/\langle g \rangle| = [G : \langle g \rangle] = \frac{|G|}{|\langle g \rangle|} = \frac{ap}{d}$$

for some integer a. Then consider $\langle h \rangle \subset G/\langle g \rangle$. This has an element of some prime order q', by the same argument, and if $q' = p$ we are done. Otherwise, we repeat this process inductively, and argue that eventually we will find an element of order p, precisely since this is a prime factor of $|G|$.

Exercise 8.18. Let G be Abelian, and $|G| = 2n$, where n is odd. It has at least one element of order 2 by the previous exercise. Now, suppose $|g| = |h| = 2$. Then $\langle g \rangle$ is a subgroup of order 2, and $|G/\langle g \rangle| = n$ by Lagrange's theorem. If $h \neq g$, we can then consider $(G/\langle g\rangle)/\langle h\rangle$ (the first quotient only deletes the element g). Applying Lagrange's theorem again, this quotient has order $n/2$. But n is odd, so this is not possible. Therefore there cannot be more than one element of order 2.

Exercise 8.19. Let G be finite and d be a proper divisor of $|G|$. If there is no element of G of order d, by Exercise 17 d cannot be prime. ???

Exercise 8.20. Let G be finite and Abelian, and d a divisor of $|G|$. If $|G| = 1$, it is trivially true that G has a subgroup H of order d for each divisor of $|G|$. Then suppose that $|G| = n$, and that we know that this is true for all finite Abelian groups of order $k < n$. Then we can write $d = kp$ for a prime p and integer $k < n$. By Exercise 17, we then have that there is an element of order p, and therefore it generates a subgroup of order p. If this element is g, this is $\langle g\rangle$, and since G is Abelian $\langle g\rangle$ is normal in G and hence we can form $G/\langle g\rangle$, which has order $|G|/|\langle g\rangle| = n/p = d$ by Lagrange's theorem. Then by induction we have that any finite Abelian group has subgroups of all proper divisor orders.

Exercise 8.21. Let H, K be subgroups of a group G. Then we have quotients

$$H/K = \{hK \mid h \in H\}$$
$$H/H \cap K = \{hH \cap K \mid h \in H\}$$

Define $\phi : H/K \to H/H \cap K$ by

$$\phi(hK) = hH \cap K$$

Then, if $\phi(hK) = \phi(h'K)$, we have $hH \cap K = h'h \cap K$ which implies that both h and h' are in K. But then $hK = h'K = eK$, so ϕ is injective. On the other hand, it is clear that it is surjective. Therefore it is a bijection. We have already seen that if H and K are finite and normal in G, HK is a subgroup of G, with

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

This is true of sets regardless of whether H and K are normal.

Exercise 8.22. This generalisation from Ab to Grp is fairly straightforward: since $\operatorname{Im}\phi$ is not necessarily normal in G' we should naturally think of the smallest normal subgroup N of G' containing $\operatorname{Im}\phi$. Then suppose $n \in G' \setminus \operatorname{Im}\phi$. It is projected by the quotient homomorphism to the trivial element in G'/N, and hence by any homomorphism $\overline{\alpha} : G'/N \to L$ to the trivial element in L. That is, it is in the kernel of α. So $N \subseteq \ker\alpha$, and we proceed as in the Abelian case. Obviously N should not be bigger than this, since this would break the uniqueness of $\overline{\alpha}$.

Exercise 8.23. Let H be the subgroup of S_3 consisting of the identity and the permutation of 1 and 2. If $\iota : H \hookrightarrow S_3$ is the inclusion, $\operatorname{coker} \iota = S_3/N$, where N is the smallest normal subgroup of S_3 containing H. But there are only three normal subgroups of S_3, $\{e\}$, A_3, and S_3 itself. But $H \not\subseteq A_3$, so $N = S_3$, and hence $\operatorname{coker} \iota = \{e\}$. Note that in Ab this would imply that ι is surjective; this is not the case here.

Exercise 8.24. We have just seen a demonstration of how Proposition **??** fails for non-Abelian groups. Specifically, $\operatorname{coker} \phi$ trivial $\Rightarrow$ ϕ surjective fails, while ϕ epic $\Rightarrow$ $\operatorname{coker} \phi$ trivial and ϕ surjective survive. So we no longer have that ϕ epic $\Rightarrow$ ϕ surjective, which is of course the statement that ϕ has right-inverses.

Exercise 8.25. Let H be a commutative normal subgroup of G. In Exercise 7.10 we defined a homomorphism $\phi : \operatorname{Inn}(G) \to \operatorname{Aut}(H)$ by

$$(\phi(\gamma_g))(h) = ghg^{-1}$$

where γ_g is the inner automorphism defined by

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

Now, we can define a homomorphism $f : G \to \operatorname{Inn}(G)$ by $f(g) = \gamma_g$. Then we can define a homomorphism $f' : G/H \to \operatorname{Aut}(H)$ by $f' = \phi \circ f$.

9 Group Actions

Exercise 9.1. We let matrix groups have the obvious left-action on Euclidean spaces.

(i) Let $v \in \mathbb{R}^n$ and $M \in O(n)$. Then $|Mv|^2 = v^T M^T M v = v^T v = |v|^2$, so $O(n)$ preserves lengths. Let also $w \in \mathbb{R}^n$, and θ be the angle between v and w, i.e.

$$\cos\theta = \frac{v \cdot w}{|v||w|}$$

The denominator is invariant under $O(n)$ as we have just seen, and $v \cdot w = v^T w$ becomes $v^T M^T M w = v^T w$, so the numerator is invariant too. Thus $O(n)$ also preserves angles.

(ii) In Exercise 8.9 we constructed a homomorphism $SU(2) \to SO(3)$,

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = \begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

Since we have an obvious action of $SO(3)$ on $\mathbb{R}^3$, this gives us an action of $SU(2)$ on $\mathbb{R}^3$. Specifically, this map induces an action of $SU(2)$ because it is a homomorphism and matrix multiplication is associative.

Exercise 9.2. Define the action $D_8 \times \mathbb{R}^2 \to \mathbb{R}^2$ by

$$\rho(x^n, v) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^n v$$
$$\rho(y^n, v) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^n v$$

where $|x| = 2$ and $|y| = 4$ are the generators of D_8. Then indeed

$$\rho(e_G, v) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^0 v = v$$

and

$$\begin{aligned} \rho(x^n y^m, v) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^m v \\ &= \rho(x^n, \rho(y^m, v)) \end{aligned}$$

which, given the relations defining D_8, is sufficient to confirm that this is an action.

Exercise 9.3. Given a group $G = (G, \cdot)$, define the opposite group $G^\circ = (G, \circ)$ by $g \circ h = h \cdot g$.

(i) Closure under $\circ$ and the existence of a unit element and inverses are clearly inherited from G. To check associativity, we have

$$\begin{aligned} (g \circ h) \circ k &= (h \cdot g) \circ k \\ &= k \cdot (h \cdot g) \\ &= (k \cdot h) \cdot g \\ &= g \circ (k \cdot g) \\ &= g \circ (h \circ k) \end{aligned}$$

So G° is indeed a group.

(ii) Consider the 'identity', $G^\circ \to G$, $g \mapsto g$. Obviously this is a bijection. Then, $\mathrm{id}(g \circ g') = g' \cdot g$, so this is only a homomorphism, and hence an isomorphism, if $\mathrm{id}\, g \cdot \mathrm{id}\, g' = \mathrm{id}\, g' \cdot \mathrm{id}\, g$ for all g, g', i.e. if G and hence G° are Abelian.

(iii) However, we can also define $\phi : G^\circ \to G$ by $\phi(g) = g^{-1}$. This is also obviously a bijection, and now we have

$$\begin{aligned}\phi(g_1 \circ g_2) &= (g_2 \cdot g_1)^{-1} \\ &= g_1^{-1} \cdot g_2^{-1} \\ &= \phi(g_1) \cdot \phi(g_2)\end{aligned}$$

So this is a homomorphism regardless of commutativity, so $G \cong G^\circ$ anyway.

(iv) It is now fairly clear that the right-action of G is equivalent to the left-action of G°. In the Abelian case, given a right-action of G on a set A ag, we can define the corresponding left-action of G° by ga, but, as we have seen, in general we should use $g^{-1}a$.

Exercise 9.4. The right-action corresponding to the obvious left-action of a group on itself by left-multiplication is, in the non-Abelian general case as discussed in the previous exercise, defined by

$$\rho(g, a) = a, g^{-1}$$

Indeed, $\rho(e_G, a) = a$, and

$$\begin{aligned}\rho(gh, a) &= a(gh)^{-1} \\ &= ah^{-1}g^{-1} \\ &= \rho(g, \rho(h, a))\end{aligned}$$

So this is an action.

Exercise 9.5. The action of a group on itself given by left-multiplication is obviously free, since if $gh = h$, $g = e_G$.

Exercise 9.6. An orbit of $a \in A$ under action of G looks like $O = \{ga \mid g \in G\}$, so if $b \in O$, $b = ga$ for some g, so the induced action of G on O is transitive.

Exercise 9.7. We have $\mathrm{Stab}_G(a) = \{g \in G \mid ga = a\}$. Let $g, h \in \mathrm{Stab}_G(a)$. Then $ga = a$ and $ha = a$. We have $e_G a = a$, so $h^{-1}ha = a$, and hence $h^{-1}a = a$. Then

$$(gh^{-1})a = ga = a$$

Therefore $\mathrm{Stab}_G(a)$ is indeed a subgroup of G.

Exercise 9.8. Knowing that Set is a category, to show that G-Set is a category all we have to do is show that equivariance is compatible with the notion of a morphism. Firstly, if $\phi : A \to B$ and $\psi : B \to C$ are equivariant, then

$$\begin{aligned} g\psi(\phi(a)) &= \psi(g\phi(a)) \\ &= \psi(\phi(ga)) \end{aligned}$$

so $\psi \circ \phi$ is equivariant, and we can use the usual composition of set-functions. Then associativity and the existence of identity morphisms quickly follow, and we have a category. Clearly isomorphisms in G-Set must be bijections, since this is what defines an isomorphism in Set. Equivariance is clearly required for commutativity of diagrams.

Exercise 9.9.

(i) Products in Set are Cartesian products, so we will try to show that the same is true in G-Set. Given sets A, B, we have $A \times B$ and projections $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$. Clearly projections may be defined to be equivariant, i.e.

$$g\pi_A(a) = \pi_A(ga)$$

and similarly for π_B, since the action of G is defined on both A and B independently, so $ga \in A$ and $gb \in B$. Now, given a set Z and morphisms $f_A : Z \to A$ and $f_B : Z \to B$, we know from Set that there is a unique set-function $\sigma : Z \to A \times B$ making

$$\begin{tikzcd}
& & A \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "f_A"] \arrow[drr, bend right, "f_B"'] & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"] & \\
& & B
\end{tikzcd}$$

commute, defined by

$$\sigma(z) = (f_A(z), f_B(z))$$

But then if f_A and f_B are equivariant, so is σ, and hence σ is a morphism in G-Set and therefore we have products.

(ii) Similarly, coproducts in Set are disjoint unions, so we will try to show the same is true in G-Set. Given sets A, B, we have $A \sqcup B$ and inclusions $\iota_A \hookrightarrow A \sqcup B$ and $\iota_B : B \hookrightarrow A \sqcup B$. Again, since the action of G is defined on A and B independently, these inclusions can be defined to be equivariant. Now, given a set Z and morphisms $f_A : A \to Z$ and $f_B : B \to Z$, we know from Set that there is a unique set-function $\sigma : A \sqcup B \to Z$ making

$$\begin{tikzcd}
A \arrow[dr, hook, "\iota_A"] \arrow[drr, bend left, "f_A"] & & \\
& A \sqcup B \arrow[r, "\sigma"] & Z \\
B \arrow[ur, hook, "\iota_B"] \arrow[urr, bend right, "f_B"] & &
\end{tikzcd}$$

commute, defined by

$$\sigma(c) = \begin{cases} f_A(c) & c \in A \\ f_B(c) & c \in B \end{cases}$$

But then if f_A and f_B are equivariant, so is σ, and hence σ is a morphism in G-Set and therefore we have coproducts.

(iii) Recall that we can partition a set A into its orbits under the action of some group. We therefore want some $H \subseteq G$ such that $G/H \cong O_G(a)$ for some $a \in A$. Every $g \in \operatorname{Stab}_G(a)$ gets sent to the trivial element in $G/\operatorname{Stab}_G(a)$, and hence the non-trivial elements in $G/\operatorname{Stab}_G(a)$ can be identified as those $g \in G$ such that $ga \neq a$. Therefore we can make the identification $G/\operatorname{Stab}_G(a) \cong O_G(a)$ as desired. Then if A is finite it can be regarded as a disjoint union of finitely many $G/\operatorname{Stab}_G(a)$, one for each orbit, and as we have just seen, the disjoint union is the coproduct in G-Set. G naturally acts on $G/\operatorname{Stab}_G(a)$ by left-multiplication.

Exercise 9.10. Let H be a subgroup of G. Then recalling Exercise 9.3, define $\phi : G/H \to H\backslash G$ by

$$\phi(gH) = Hg^{-1}$$

This is a bijection.

Exercise 9.11. Let G be finite, and H a subgroup of G of order p, the smallest prime dividing $|G|$. Regard the action of G on G/H by left-multiplication as a homomorphism $\sigma : G \to S_p$. Then $G/\ker\sigma \cong \operatorname{Im}\sigma \subseteq S_p$. But then $|\operatorname{Im}\sigma|$ divides $|S_p| = p!$, so we can write $p! = n|\operatorname{Im}\sigma|$. We then have

$$|\ker\sigma| = \frac{|G|}{|\operatorname{Im}\sigma|} = \frac{mn}{(p-1)!}$$

where we have written $|G| = mp$. Now, suppose $g \in \ker\sigma$. Then g should correspond to the trivial element of G/H, so $g \in H$. Therefore $\ker\sigma \subseteq H$, so $|\ker\sigma|$ must divide $|H| = p$. Therefore $|\ker\sigma| = 1$ or p. In the latter case, $\ker\sigma \subseteq H$ and has the same order, so $\ker\sigma = H$. So since all kernels are normal, H is normal. On the other hand, if $|\ker\sigma| = 1$, so $\ker\sigma = e_G$, and hence σ is injective. But then e_G is the only element whose action (regarded as left-multiplication) on G/H is trivial, so it is the only element of G in H. Then $|H| = 1$, but by hypothesis $|H| > 1$, so this case does not exist. Then $\ker\sigma = H$ and we are done.

Exercise 9.12. Let $H \subseteq G$, $|H| = n$. Then in the same way as the previous question we can define $\sigma : G \to S_n$, so $G/\ker\sigma \cong \operatorname{Im}\sigma \subseteq S_n$. Then $|\operatorname{Im}\sigma|$ divides $n!$, i.e. $|\operatorname{Im}\sigma|m = n!$, and $\ker\sigma$ is a normal subgroup of G. Then we have

$$\begin{aligned}\frac{|G|}{|\ker\sigma|} &= \frac{n!}{m}\\ [G : \ker\sigma] &= \frac{n!}{m}\end{aligned}$$

Then stuck?

Exercise 9.13. Let $H \subseteq G$ be any subgroup, and $g \in G$ any element. Then we have the quotients (at least as sets) $G/H = \{g'H \mid g' \in G\}$ and $G/(gHg^{-1}) = \{g'(gHg^{-1}) \mid g'inG\}$. Clearly $H \cong gHg^{-1}$ as sets (by $h \mapsto ghg^{-1}$, so there must exist a corresponding bijection $G/H \to G/(gHg^{-1})$. Define $\phi : G/H \to G/(gHg^{-1})$ by

$$\phi(g'H) = g'(gHg^{-1})$$

This is clearly surjective. Then since they are isomorphic as sets $|G/H| = |G/(gHg^{-1})|$, so surjectivity implies injectivity, and hence bijectivity. Then we just need to check equivariance under left-multiplication. Indeed,

$$\begin{aligned}\phi(g''(g'H)) &= \phi((g''g')H)\\ &= (g''g')(gHg^{-1})\\ &= g''(g')(gHg^{-1})\end{aligned}$$

Thus ϕ is an isomorphism in G-Set.

Exercise 9.14. The modular group $PSL(2;\mathbb{Z})$ is generated by

$$x = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \quad y = \begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}$$

which satisfy the relations $x^2 = y^3 = e$. If there are no further relations, it has presentation $(x, y \mid x^2, y^3)$, and hence is just the coproduct $C_2 * C_3$. We want to show this is the case. From x, we just have x itself, since $x^0 = x^2 = e$ and $x^{-1} = x$. From y, we have $y^{\pm 1}$ since $y^0 = y^3 = e$, so $y^2 = y^{-1}$. So a generic element of $PSL(2;\mathbb{Z})$ is a product

$$(y^{\pm 1}x)(y^{\pm 1}x)...(y^{\pm 1}x)$$

or

$$(y^{\pm 1}x)(y^{\pm 1}x)...(y^{\pm 1}x)y^{\pm 1}$$

We want to show that these are never equal to the identity if there is more than one factor in brackets. To see this, define an action on the set of irrational reals by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(r) = \frac{ar+b}{cr+d}$$

Indeed, the RHS is irrational, clearly the action of I_2 is trivial, and

$$\begin{aligned}
\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c & d' \end{pmatrix}\right](r) &= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}(r) \\
&= \frac{(aa'+bc')r+(ab'+bd')}{(ca'+dc')r+(cb'+dd')} \\
&= \frac{a(a'r+b')+b(c'r+d)}{c(a'r+b')+d(c'r+d')} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\frac{a'r+b}{c'r+d}\right) \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}(r)\right]
\end{aligned}$$

We have

$$\begin{aligned}
y(r) &= 1-\frac{1}{r} \\
y^{-1}(r) = y^2(r) &= y\left(1-\frac{1}{r}\right) = 1-\frac{1}{r}-\left(1-\frac{1}{r}\right)^{-1} = \frac{1}{1-r} \\
x(r) &= -\frac{1}{r} \\
yx(r) &= 1-\left(-\frac{1}{r}\right)^{-1} = 1+r \\
y^{-1}x(r) = y^2x(r) &= y(1+r) = 1-(1+r)^{-1} = \frac{r}{1+r}
\end{aligned}$$

So both yx and $y^{-1}x$ send positive irrationals to positive irrationals. However, y sends any $r \in (0,1)$ to a negative irrational, so $(y^{\pm 1}x)(y^{\pm 1}x)...(y^{\pm 1}x)y$ cannot be the identity on the irrationals, and therefore cannot be the identity in $PSL(2;\mathbb{Z})$. Now we just have to check if any combination $(y^{\pm 1}x)(y^{\pm 1}x)...(y^{\pm 1}x)$ acts as the identity. $yx(r) > r$, and if we take $r \in (0,1)$, $y^{-1}x(r) > r$ as well, so no repeated application of them can return r for any $r \in (0,1)$, and hence $(y^{\pm 1}x)(y^{\pm 1}x)...(y^{\pm 1}x)$ cannot act as the identity on the irrationals, and cannot be the identity in $PSL(2;\mathbb{Z})$.

Exercise 9.15. Consider the action of a group G on the associated Cayley graph, such that if vertices v_1 and v_2 are connected by a (directed) edge, so are gv_1 and gv_2 for all $g \in G$. Then if $gv = v$, all the vertices connected by an edge to v would also have to be invariant, and thus the entire connected component including v would have to be invariant. But then this is the action of e_G only. So the action is free. In Exercise 8.6 we proved that a they associated Cayley graph of a (finite) freely generated group is a tree, so here we have that every (finite) free group acts freely on a tree, namely its associated Cayley graph.

Exercise 9.16. It is also true that only free groups act freely on trees. Therefore a group acts freely on trees iff it is a free group. It is clear that given the (free) action of a free group on a tree, the induced action of any subgroup on the tree must also be free. Therefore all subgroups of free groups (on finite sets) are free.

Exercise 9.17. We can regard $G \in \mathrm{Obj}(G\text{-}\mathsf{Set}$, by the action on the underlying set of left-multiplication. Then every automorphism in G-Set is an equivariant bijection $G \to G$ given by left-multiplication. That is, each $\phi \in \mathrm{Aut}_{G-\mathsf{Set}}(G)$ is defined by $\phi(g) = g'g$ for some $g' \in G$. So clearly $\mathrm{Aut}_{G-\mathsf{Set}}(G) \cong G$.

Exercise 9.18. Recall that a groupoid is a category in which every morphism is an isomorphism. Define a category to have objects a, the elements of a set A upon which we act with G. Given an action of G on A and $a, b \in A$ we define $\mathrm{Hom}(a, b) = \{g \mid \rho(g, a) = b\}$. That is, for each pair (a, b) of elements of A, the only morphism, if it exists, is defined by the action of an element g taking a to b. Then by the definition of ρ, the composition is associative, and we have identity morphisms since $\mathrm{Hom}(a, a) = \{e_G\}$. Then we have a groupoid encoding the action of G on A.

10 Group Objects in Categories

Exercise 10.1. In the associativity diagram, the isomorphism is defined by $((g_1, g_2), g_3) \mapsto (g_1, (g_2, g_3))$. We saw that this was an isomorphism in Exercise 1.5.9.

The isomorphism in the left-identity diagram is $m \circ (e \times \mathrm{id}_G)$. If ϵ is the unique morphism $G \to 1$, we have $\epsilon \times \mathrm{id}_G : G \to 1 \times G$. Then we observe that $(\epsilon \times \mathrm{id}_G) \circ m \circ (e \times \mathrm{id}_G)$ is the identity. Similarly the isomorphism in the right-identity diagram.

The unlabelled morphisms in the inverse diagrams are the unique morphisms $\epsilon : G \to 1$.

Exercise 10.2. It is easy to check that group objects in Set are exactly groups as usually defined. The existence of $m : G \times G \to G$ tells us that the group is closed under the product. The first diagram tells us the product is associative. The second and third diagram tells us there exists an element that is both a left- and right-identity. The fourth and fifth diagram tells us that to each element corresponds another, which is both a left- and a right-identity.

Exercise 10.3. Let $(G, \cdot)$ be a group, and $\circ : G \times G \to G$ a homomorphism wrt $\circ$ such that $(G, \circ)$ is also a group. Homomorphisms map trivial elements to each other, so the identities are the same. But then inverses, and the operations themselves will be the same.

Exercise 10.4. A group object in Ab is an Abelian group G together with homomorphisms $m : G \times G \to G$, $e : \{e\} \to G$, $i : G \to G$, where $\{e\}$ is the trivial group. But m, e, i are all specified by the choice of group. Therefore the group object structure we can put on G is unique.

Exercise 10.5. Generalising to Grp, we notice that $i : G \to G$ being a homomorphism means $g_1^{-1} g_2^{-1} = g_2^{-1} g_1^{-1}$ for all $g_1, g_2 \in G$, that is, G must be Abelian. So group objects in Grp are Abelian groups.