Chapter 2

Exercises on Group Theory

Exercises marked by (*) are considered difficult. Exercises marked by (**) were previous midterm/exam questions.

2.1 Groups and subgroups

Exercise 1. *a*) Show the unicity of the identity element in a group.

b) For g an element in a group G, show the unicity of its inverse.

Answer.

a) Suppose that we have two identities e and e'. Then $ee' = e'$ because e is an identity, but also $ee' = e$ because e' is an identity, and therefore $e = e'$.

b) Let g be an element in G. Suppose it has two inverses g^{-1} and $(g')^{-1}$. Then $gg^{-1} = 1 = g(g')^{-1}$. Thus $g^{-1}(gg^{-1}) = g^{-1} = (g^{-1}g)(g')^{-1}$ and $g^{-1} = (g')^{-1}$.

Exercise 2. Let G be a group and let H be a nonempty subset of G. Prove that the following are equivalent by proving 1. $\Rightarrow$ 3. $\Rightarrow$ 2. $\Rightarrow$ 1.:

1. H is a subgroup of G.
2. (a) $x, y \in H$ implies $xy \in H$ for all x, y.
   (b) $x \in H$ implies $x^{-1} \in H$.
3. $x, y \in H$ implies $xy^{-1} \in H$ for all x, y.

Now that we have seen that the two following statements are equivalent:

a) H is a subgroup of G,

b) b_1) $x, y \in H \Rightarrow xy \in H$

$b_2)$ $x \in H \Rightarrow x^{-1} \in H$.

1. Show that $b_1)$ is not sufficient to show that H is a subgroup of G.

2. Show that however, if G is a finite group, then $b_1)$ is sufficient.

Answer. We prove that 1. $\Rightarrow$ 3. $\Rightarrow$ 2. $\Rightarrow$ 1.

1. $\Rightarrow$ 3. This part is clear from the definition of subgroup.

3. $\Rightarrow$ 2. Since H is non-empty, let $x \in H$. By assumption of 3., we have that $xx^{-1} = 1 \in H$ and that $1x^{-1} \in H$ thus x is invertible in H. We now know that for $x, y \in H$, x and y^{-1} are in H, thus $x(y^{-1})^{-1} = xy$ is in H.

2. $\Rightarrow$ 1. To prove this direction, we need to check the definition of group. Since closure and existence of an inverse are true by assumption of 2., and that associativity follows from the associativity in G, we are left with the existence of an identity. Now, if $x \in H$, then $x^{-1} \in H$ by assumption of 2., and thus $xx^{-1} = 1 \in H$ again by assumption of 2., which completes the proof.

Now for the second part of the exercise:

1. Consider for example the group $G = \mathbb{Q}^*$ with multiplication. Then the set $\mathbb{Z}^*$ with multiplication satisfies that if $x, y \in \mathbb{Z}$ then $xy \in \mathbb{Z}$. However, $\mathbb{Z}$ is not a group with respect to multiplication since $2 \in \mathbb{Z}$ but $1/2$ is not in $\mathbb{Z}$.

2. Let $x \in H$. Then take the powers $x, x^2, x^3, \ldots$ of x. Since G is finite, there is some n such that $x^n = 1$, and by $b_1)$, $x^n \in H$ thus $1 \in H$, and $x^{n-1} = x^{-1} \in H$.

Exercise 3. Let G be a finite group of order n such that all its non-trivial elements have order 2.

1. Show that G is abelian.

2. Let H be a subgroup of G, and let $g \in G$ but not in H. Show that $H \cup gH$ is a subgroup of G.

3. Show that the subgroup $H \cup gH$ has order twice the order of H.

4. Deduce from the previous steps that the order of G is a power of 2.

Answer.

1. Let $x, y \in G$, x, y not 1. By assumption, $x^2 = y^2 = 1$, which also means that x, y and xy are their own inverse. Now

$$(xy)(xy) = 1 \Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

2. First note that $H \cup gH$ contains 1 since $1 \in H$. Let $x, y \in H \cup gH$. Then $x \in H$ or $x \in gH$, and $y \in H$ or $y \in gH$. If both $x, y \in H$, then clearly $xy \in H$ since H is a subgroup. If both $x, y \in gH$, then $x = gh, y = gh'$ and $xy = ghgh' = hh' \in H$ since G is commutative and $g^2 = 1$. If say $x \in H$ and $y \in gH$ (same proof vice-versa), then $xy = xgh = g(xh) \in gH$ since G is commutative. For the inverse, if $x \in H$, then $x^{-1} \in H$ since H is a subgroup. If $x \in gH$, then $x = gh$, and $x^{-1} = h^{-1}g^{-1} = gh$ since G is commutative and all elements have order 2.

3. It is enough to show that the intersection of H and gH is empty. Let $x \in H$ and $x \in gH$. Then $x = gh$ for $h \in H$, so that $xh = gh^2 = g$, which is a contradiction, since $xh \in H$ and g is not in H by assumption.

4. Take h an element of order 2 in G, and take $H = \{1, h\}$. If $G = H$ we are done. If not, there is a g not in H, and by the previous point $H \cup gH$ has order 4. We can now iterate. If $G = H \cup gH$ we are done. Otherwise, $H \cup gH = H'$ is a subgroup of G, and there exists a g' not in H', so that $H' \cup g'H'$ has order 8. One can also write a nice formal proof by induction.

Exercise 4. Let G be a group and let H and K be two subgroups of G.

1. Is $H \cap K$ a subgroup of G? If your answer is yes, prove it. If your answer is no, provide a counterexample.

2. Is $H \cup K$ a subgroup of G? If your answer is yes, prove it. If your answer is no, provide a counterexample.

Answer.

1. This is true. It is enough to check that $xy^{-1} \in H \cap K$ for $x, y \in H \cap K$. But since $x, y \in H$, we have $xy^{-1} \in H$ since H is a subgroup, and likewise, $xy^{-1} \in K$ for $x, y \in K$ since K is a subgroup.

2. This is false. For example, take the group $\mathbb{Z}$ with subgroups $3\mathbb{Z}$ and $2\mathbb{Z}$. Then 2 and 3 are in their union, but 5 is not.

Exercise 5. Show that if G has only one element of order 2, then this element is in the center of G (that is the elements of G which commute with every element in G).

Answer. Let x be the element of order 2. Then for any y, yxy^{-1} is such that $(yxy^{-1})(yxy^{-1}) = 1$. Thus the order of yxy^{-1} is either 1 or 2, that is, yxy^{-1} must be either 1 or x. If $yxy^{-1} = 1$, then $x = 1$ a contradiction. Thus $yxy^{-1} = x$.

Exercise 6. Let G be a group and H be a subgroup of G. Show that

$$N_G(H) = \{g \in G,\ gH = Hg\}$$

and

$$C_G(H) = \{g \in G,\ gh = hg \text{ for all } h \in H\}$$

are subgroups of G.

Answer. Take $x, y \in N_G(H)$. We have to check that $xy^{-1} \in N_G(H)$, that is, that $xy^{-1}H = Hxy^{-1}$. But $Hxy^{-1} = xHy^{-1}$ since $x \in N_G(H)$, and $xHy^{-1} = xy^{-1}H$ since $yH = Hy \iff y^{-1}H = Hy^{-1}$.

Now take $x, y \in C_G(H)$. We have to check that $xy^{-1}h = hxy^{-1}$ for all $h \in H$. But $hxy^{-1} = xhy^{-1}$ because $x \in C_G(H)$, and $xhy^{-1} = xy^{-1}h$ since $yh = hy \iff y^{-1}h = hy^{-1}$.

Exercise 7. Let $G = \mathbb{Z}_{20}^*$ be the group of invertible elements in $\mathbb{Z}_{20}$. Find two subgroups of order 4 in G, one that is cyclic and one that is not cyclic.

Answer. The group G contains

$$|G| = \varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8.$$

These 8 elements are coprime to 20, that is

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

The subgroup

$$\langle 3 \rangle = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 21 = 1\}$$

is cyclic of order 4. We have that

$$11, 11^2 = 121 = 1, 19, 19^2 = (-1)^2 = 1, 11 \cdot 19 = (-11) = 9, 9^2 = 81 = 1$$

and

$$\{1, 11, 19, 9\}$$

is a group of order 4 which is not cyclic.

2.2 Cosets and Lagrange's Theorem

Exercise 8. Let $G = S_3$ be the group of permutations of 3 elements, that is

$$G = \{(1), (12), (13), (23), (123), (132)\}$$

and let $H = \{(1), (12)\}$ be a subgroup. Compute the left and right cosets of H.

Answer. We have

g	gH	Hg
(1)	$\{(1), (12)\}$	$\{(1), (12)\}$
(12)	$\{(1), (12)\}$	$\{(1), (12)\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(13), (123)\}$	$\{(23), (123)\}$
(132)	$\{(23), (132)\}$	$\{(13), (132)\}$

For example, $H(23)$ is $\{(1)(23), (12)(23)\}$. Clearly $(1)(23) = (23)$. Now $(12)(23)$ sends $123 \mapsto 132$ via (23), and then sends $132 \mapsto 231$ via (12), so that finally we have $123 \mapsto 231$ which can be written (123).

Exercise 9. Let G be a finite group and let H and K be subgroups with relatively prime order. Then $H \cap K = \{1\}$.

Answer. Since $H \cap K$ is a subgroup of both H and K, we have

$$|H \cap K| \mid |H|, \ |H \cap K| \mid |K|$$

by Lagrange's Theorem. Since $(|H|, |K|) = 1$, it must be that $|H \cap K| = 1$ implying that $H \cap K = \{1\}$.

Exercise 10. (**) Let G be a finite group, and let H and K be subgroups G.

1. Show that $H \cap K$ is a subgroup of H.
2. Since $H \cap K$ is a subgroup of H, we consider the set of distinct left cosets of $H \cap K$ in H, given by $\{h_1(H \cap K), \ldots, h_r(H \cap K)\}$ for some $h_1, \ldots, h_r \in H$. For any element $hk \in HK$, show that $hk \in h_i K$.
3. Prove that the left cosets $h_1 K, \ldots, h_r K$ of K in HK are all disjoint (I would suggest to do it by contradiction).
4. Deduce from the above steps that

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

Answer.

1. Since $a, b \in H \cap K$, then $a, b \in H$ and $a, b \in K$ and both H and K are subgroups, so it must be that $ab^{-1} \in H$ and $ab^{-1} \in K$. Thus $ab^{-1} \in H \cap K$, which is a subgroup, contained in H by definition.
2. For any element $hk \in HK$, since the union of the r cosets give H, $h = h_i g$ for some element $g \in H \cap K$. Then $hk = h_i gk = h_i(gk) \in h_i K$ since both k and g belong to the subgroup K.
3. Suppose by contradiction that there are some h_i, h_j for which $h_i K = h_j K$. But then this would mean that $h_j^{-1} h_i \in K$. Now since we also have $h_j^{-1} h_i \in H$, this would imply that $h_j^{-1} h_i \in H \cap K$, that is $h_i(H \cap K) = h_j(H \cap K)$, which cannot happen since these cosets are distinct.
4. From the above, we know from 2. that

$$r = \frac{|H|}{|H \cap K|}.$$

Then from 4., we know that

$$r = \frac{|HK|}{|K|}.$$

This is because the cosets are forced to be distinct, and there cannot have more than r of them since in 3., every hk belongs to one of the h_iK. Thus

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

2.3 Normal subgroups and quotient group

Exercise 11. Consider the following two sets:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, c \in \mathbb{R}^*,\ b \in \mathbb{R} \right\},\ U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in \mathbb{R} \right\}.$$

1. Show that T is a subgroup of $GL_2(\mathbb{R})$.
2. Show that U is a normal subgroup of T.

Answer.

1. It is enough to show that if $X, Y \in T$, then $XY^{-1} \in T$. Let

$$X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ Y = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

then

$$XY^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} = \frac{1}{a'c'} \begin{pmatrix} ac' & -ab' + a'b \\ 0 & a'c \end{pmatrix} \in T$$

2. We have to show that $XYX^{-1} \in U$ when $Y \in U$ and $X \in T$. We have

$$\begin{aligned} XYX^{-1} &= \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \begin{pmatrix} a' & a'b + b' \\ 0 & c' \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \frac{1}{a'c'} \begin{pmatrix} a'c' & -b'a' + a'(a'b + b') \\ 0 & a'c' \end{pmatrix} \in U. \end{aligned}$$

Exercise 12. Let G be a group, and let H be a subgroup of index 2. Show that H is normal in G.

Answer. If H is of index 2, that means by definition that there are only 2 cosets, say H and g_1H for some g_1 not in H. Note that if $g_1 \neq g_2 \in G$ are not

in H,then $g_1g_2 \in H$. Indeed, we have that either $g_1g_2 \in H$ or $g_1g_2 \in g_1H$ (recall that the cosets partition the group), and $g_1g_2 \in g_1H$ is not possible since g_2 is not in H. In other words, if both g_1, g_2 are not in H, then $(g_1g_2)H(g_1g_2)^{-1} \in H$.

Now let $h \in H$, $g \in G$. If $g \in H$, then $ghg^{-1} \in H$ and we are done. If g is not in H, then gh is not in H and by the above remark we have that $ghg^{-1} = (gh)g^{-1} \in H$ (take $g_1 = gh, g_2 = g^{-1}$). Alternatively by the same above remark, since $(g_1g_2)H(g_1g_2)^{-1} \in H$ for every g_1, g_2 not in H, it is enough to wrote g as g_1g_2, say $g_1 = g$ (g is not in H) and $g_2 = g^{-1}h$ (which is not in H either).

Exercise 13. (*) If G_1 is normal in G_2 and G_2 is normal in G_3, then G_1 is normal in G_3. True or false?

Answer. This is wrong (it takes the notion of *characteristic subgroup* to get transitivity). An example is the dihedral group D_4:

$$D_4 = \langle r, f | f^2 = 1, r^4 = 1, fr = r^{-1}f \rangle.$$

The subgroup

$$H = \langle rf, fr \rangle = \{1, rf, r^2, fr\} \simeq C_2 \times C_2$$

is isomorphic to the Klein group. We have that $H \lhd G$. Finally

$$K = \langle rf \rangle = \{1, rf\} \lhd H$$

but K is not normal in G, since $f \cdot rf \cdot f^{-1} = f \cdot rf \cdot f = fr$ which is not in K.

Exercise 14. Let G be a group and let $Z(G)$ be its center (that is the elements of G which commute with every element in G). Show that if $G/Z(G)$ is cyclic then G is abelian. Give an example to show that if $G/Z(G)$ is only abelian, then G does not have to be abelian.

Answer. If $G/Z(G)$ is cyclic, then $G/Z(G) = \langle gZ(G) \rangle$. Let $x, y \in G$, then their corresponding cosets are $xZ(G), yZ(G)$ which can be written

$$xZ(G) = (gZ(G))^k = g^kZ(G),\ yZ(G) = (gZ(G))^l = g^lZ(G)$$

and

$$x = g^kz_1,\ y = g^lz_2,\ z_1, z_2 \in Z(G).$$

Now

$$xy = g^kz_1g^lz_2 = yx$$

since $z_1, z_2 \in Z(G)$. For example, consider the dihedral group $D_4 = \{r, f | f^2 = 1, r^4 = 1, fr = r^{-1}f\} = \{1, r, r^2, r^3, f, rf, r^2f, r^3f\}$. Its center is $Z(D_4) = \{1, r^2\}$: indeed, r cannot be in the center since $fr = r^{-1}f$, then r^2 commutes with r^i for all i, and r^2 commutes with f since $fr^2 = (fr)r = r^{-1}fr = r^{-2}f = r^2f$, so r^2 is in the center. This also shows that r^3 cannot be inside since r is not. Then f cannot be in the center since $fr = r^{-1}f$, and fr cannot be either

since $(fr)f = r^{-1}ff = r^{-1}$ while $ffr = r$. Then fr^2 cannot be since f is not and r^2 is, fr^3 cannot be since fr is not and r^2 is. Thus $D_4/Z(D_4)$ is a group of order 4, it contains 4 cosets: $Z(D_4), rZ(D_4), fZ(D_4), rfZ(D_4)$, which is isomorphic to the Klein group, which is abelian but not cyclic. One can check directly that every element has order 2, and therefore it cannot be cyclic and it must be abelian.

Exercise 15. 1. Let G be a group. Show that if H is a normal subgroup of order 2, then H belongs to the center of G.

2. Let G be a group of order 10 with a normal subgroup H or order 2. Prove that G is abelian.

Answer.

1. Since H is of order 2, then $H = \{1, h\}$. It is furthermore normal, so that $gHg^{-1} = \{1, ghg^{-1}\}$ is in H, thus $ghg^{-1} = h$ and we are done, since this is saying that h commutes with every $g \in G$.

2. Since H is normal in G, G/H has a group structure, and $|G/H| = |G|/|H| = 10/2 = 5$. Thus the quotient group G/H is a group of order 5, implying that it is cyclic. Now take x, y in G, with respective coset xH, yH. Since the quotient group is cyclic, there exists a coset gH such that $xH = (gH)^k = g^kH$, and $yH = (gH)^l = g^lH$ for some k, l. Thus $x = g^kh$, $y = g^lh'$ for some $h, h' \in H$. We are left to check that $xy = yx$, that is $g^khg^lh' = g^lh'g^kh$, which is true since we know that $h, h' \in H$ which is contained in the center of G (by the part above).

2.4 The isomorphism theorems

Exercise 16. Consider A the set of affine maps of $\mathbb{R}$, that is

$$A = \{f : x \mapsto ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R}\}.$$

1. Show that A is a group with respect to the composition of maps.

2. Let
$$N = \{g : x \mapsto x + b,\ b \in \mathbb{R}\}.$$
Show that N is a normal subgroup of A.

3. Show that the quotient group A/N is isomorphic to $\mathbb{R}^*$.

Answer.

1. Let $f, g \in A$. Then

$$(f \circ g)(x) = f(ax + b) = a'(ax + b) + b' = a'ax + a'b + b',$$

where $a'a \in \mathbb{R}^*$ thus the closure property is satisfied. The composition of maps is associative. The identity element is given by the identity map since

$$\mathrm{Id} \circ f = f \circ \mathrm{Id} = f.$$

Finally, we need to show that every $f \in A$ is invertible. Take $f^{-1}(x) = a^{-1}x - a^{-1}b$. Then

$$f^{-1} \circ f(x) = f^{-1}(ax + b) = a^{-1}(ax + b) - a^{-1}b = x.$$

2. To show that N is a subgroup, the same above proof can be reused with $a = 1$. Let $g \in N$ and let $f \in A$. We have to show that

$$f \circ g \circ f^{-1} \in N.$$

We have

$$f \circ g(a^{-1}x - a^{-1}b) = f(a^{-1}(x) - a^{-1}b + b') = x - b + ab' + b \in N.$$

3. Define the map

$$\varphi : A \to \mathbb{R}^*,\ f(x) = ax + b \mapsto a.$$

It is a group homomorphism since

$$\varphi(f \circ g) = a'a = \varphi(f)\varphi(g).$$

The kernel of φ is N and its image is $\mathbb{R}^*$. By the 1st isomorphism theorem, we thus have that

$$A/N \simeq \mathbb{R}^*.$$

Exercise 17. Use the first isomorphism theorem to

1. show that
$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$
2. show that
$$\mathbb{C}^*/U \simeq \mathbb{R}_+^*,$$
where
$$U = \{z \in \mathbb{C}^* \mid |z| = 1\}.$$
3. compute
$$\mathbb{R}/2\pi\mathbb{Z}.$$

Answer.

1. Consider the map:

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^*,\ X \mapsto \det(X).$$

It is a group homomorphism. Its kernel is $SL_n(\mathbb{R})$, its image is $\mathbb{R}^*$ and thus by the 1st isomorphism theorem, we have

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

2. Consider the map
$$|\cdot| : \mathbb{C}^* \to \mathbb{R}_+^*,\ z \mapsto |z|.$$
It is a group homomorphism. Its kernel is U, and its image is $\mathbb{R}_+^*$ and thus by the 1st isomorphism theorem, we have
$$\mathbb{C}^*/U \simeq \mathbb{R}_+^*.$$

3. Define the map
$$f : \mathbb{R} \to \mathbb{C}^*,\ x \mapsto e^{ix}.$$
It is a group homomorphism. Its kernel is $2\pi\mathbb{Z}$. Its image is $\{e^{ix},\ x \in \mathbb{R}\} = U$. Thus by the 1st isomorphism theorem
$$\mathbb{R}/2\pi\mathbb{Z} \simeq U.$$

Exercise 18. Let $G = \langle x \rangle$ be a cyclic group of order $n \geq 1$. Let $h_x : \mathbb{Z} \to G$, $m \mapsto x^m$.

- Show that h_x is surjective and compute its kernel.
- Show that $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Answer.

- Let $g \in G$. Since $G = \langle x \rangle$, $g = x^k$ for some $0 \leq k \leq n-1$ and thus h_x is surjective. Its kernel is the set of m such that $x^m = 1$, thus m must be a multiple of n and $Ker(h_x) = n\mathbb{Z}$.
- By the 1st isomorphism theorem, since h_x is a group homomorphism, we have
$$G \simeq \mathbb{Z}/n\mathbb{Z}.$$

Exercise 19. Prove the third isomorphism theorem for groups, namely that if N and H are normal subgroups of G, with N contained in H, then
$$G/H \simeq (G/N)/(H/N).$$

Answer. This follows from the 1st isomorphism theorem for groups, if we can find an epimorphism of G/N into G/H with kernel H/N: take $f(aN) = aH$. Now f is well-defined, since if $aN = bN$, then $a^{-1}b \in N \subset H$ so $aH = bH$. Since a is arbitrary in G, f is surjective. By definition of coset multiplication, f is a homomorphism. The kernel is
$$\{aN,\ aH = H\} = \{aN,\ a \in H\} = H/N.$$

2.5 Direct and semi-direct products

Exercise 20. Let G be a group with subgroups H and K. Suppose that $G = HK$ and $H \cap K = \{1_G\}$. Then every element g of G can be written uniquely in the form hk, for $h \in H$ and $k \in K$.
Answer. Since $G = HK$, we know that g can be written as hk. Suppose it can also be written as $h'k'$. Then $hk = h'k'$ so ${h'}^{-1}h = k'k^{-1} \in H \cap K = \{1\}$. Therefore $h = h'$ and $k = k'$.

Exercise 21. The *quaternion group* Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{aligned} 1 \cdot a = a \cdot 1 = a, \ \forall\ a \in Q_8 \\ (-1) \cdot (-1) = 1, \ (-1) \cdot a = a \cdot (-1) = -a, \ \forall\ a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 \\ i \cdot j = k, \ j \cdot i = -k, \\ j \cdot k = i, \ k \cdot j = -i, \\ k \cdot i = j, \ i \cdot k = -j. \end{aligned}$$

Show that Q_8 cannot be isomorphic to a semi-direct product of smaller groups.

Answer. By definition, a semi direct product must contain two smaller subgroups of trivial intersection $\{1\}$. Now the smaller subgroups of Q_8 are $\{1, -1\}$, $\{1, i, -i, -1\}$, $\{1, j, -j, -1\}$, $\{1, k, -k, -1\}$, and each contains -1 so that it is not possible that Q_8 is a semi-direct product.

Exercise 22. Consider the set of matrices

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \ a \neq 0, \ a, b \in \mathbb{F}_p \right\}$$

(where $\mathbb{F}_p$ denotes the integers mod p).

1. Show that G is a subgroup of $SL_2(\mathbb{F}_p)$.
2. Write G as a semi-direct product.

Answer.

1. That G is a subset of $SL_2(\mathbb{F}_p)$ is clear because the determinant of every matrix in G is 1. We have to show that for $X, Y \in G$, $XY^{-1} \in G$. This is a straightforward computation:

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} c^{-1} & -d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac^{-1} & -da + bc \\ 0 & a^{-1}c \end{pmatrix} \in G.$$

2. Take

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},\ a \neq 0,\ a \in \mathbb{F}_p \right\}$$

and

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in \mathbb{F}_p \right\}.$$

Both K and H are subgroups of G. Their intersection is the 2-dimensional identity matrix, and $HK = G$, since

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a & ba^{-1} \\ 0 & a^{-1} \end{pmatrix}$$

and ba^{-1} runs through every possible element of $\mathbb{F}_p$ (since b does). Also H is normal in G, since

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2 b \\ 0 & 1 \end{pmatrix} \in H.$$

Note that K is not normal, which can be seen by doing the same computation. Thus G is the semi-direct product of H and K.

Exercise 23. Show that the group $\mathbb{Z}_n \times \mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime. Here $\mathbb{Z}_n$ denotes the integers modulo n.

Answer. If m and n are relatively prime, then for a multiple of $(1, 0)$ to be zero, it must be a multiple of n, and for a multiple of $(0, 1)$ to be zero, it must be a multiple of m. Thus for a multiple k of $(1, 1)$ to be zero, it must be a multiple of both n and m, and since they are coprime, the smallest possible value of k is mn. Hence $\mathbb{Z}_n \times \mathbb{Z}_m$ contains an element of order mn, showing that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$. Conversely, suppose that $\gcd(m, n) > 1$. Then the least common multiple of m and n is smaller than mn, let us call it d. This shows that every element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order at most d and thus none of them can generate the whole group, so that it cannot be cyclic, and thus cannot be isomorphic to $\mathbb{Z}_{mn}$.

Note that one can also prove this result by the definition of direct product: we have that $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are both normal subgroups of $\mathbb{Z}_{mn}$ because this is an abelian group. We are thus left to look at the intersection of $\mathbb{Z}_m$ and $\mathbb{Z}_n$. Recall that $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are embedded into $\mathbb{Z}_{mn}$ as respectively

$$\mathbb{Z}_m = \{0, n, 2n, \ldots, (m-1)n\},\ \mathbb{Z}_n = \{0, m, 2m, \ldots, (n-1)m\}.$$

If m and n are coprime, then $\mathbb{Z}_m \cap \mathbb{Z}_n = \{0\}$. Conversely, if x belongs to the intersection and is non-zero, then x must be a multiple of both n and m which is not congruent to 0 modulo mn, and thus m and n cannot be coprime.

Exercise 24. Let $\mathbb{Z}_3$ denote the group of integers modulo 3.

1. Show that the map

$$\sigma : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3, (x, y) \mapsto (x + y, y)$$

is an automorphism of $\mathbb{Z}_3 \times \mathbb{Z}_3$ of order 3.

2. Show that the external semi-direct product of $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_3$ by ρ, $\rho : \mathbb{Z}_3 \to Aut(\mathbb{Z}_3 \times \mathbb{Z}_3),\ i \mapsto \sigma^i$, is a non-abelian group G satisfying that

$$a^3b^3 = (ab)^3$$

for any a, b in G.

Answer.

1. So to be an automorphism, σ has to be a group homomorphism, but

$$\sigma((x+x', y+y')) = (x+x'+y+y', y+y') = (x+y, y)+(x'+y', y') = \sigma(x, y)+\sigma(x', y').$$

It clearly goes from the group to itself, and it is a bijection. It is an injection

$$\sigma(x, y) = \sigma(x', y') \Rightarrow (x + y, y) = (x' + y', y') \Rightarrow y = y', x = x',$$

and thus it is a surjection since the group is finite. It is of order 3, since

$$\sigma(x, y) = (x + y, y),\ \sigma^2(x, y) = (x + 2y, y),\ \sigma^3(x, y) = (x + 3y, y) = (x, y).$$

2. An element in the external semi-direct product is of the form $((x, y), i)$, and we have

$$((x, y), i)((x, y), i) = ((x, y) + \sigma^i(x, y), 2i),$$

$$\begin{aligned} ((x, y), i)^3 &= ((x, y) + \sigma^i(x, y) + \sigma^{2i}(x, y), 3i) \\ &= ((x, y) + (x + iy, y) + (x + 2iy, y), 3i) \\ &= ((3x + 3iy, 3y), 3i) \\ &= ((0, 0), 0). \end{aligned}$$

This shows that for any element a of the semi-direct product $a^3 = 0$, thus $b^3 = 0$, ab is another element of the group thus $(ab)^3 = 0$ which shows that $a^3b^3 = 0 = (ab)^3$, though the group is non-abelian (because σ is not the identity).

Exercise 25. (**)

1. Given a group G and a subgroup H, suppose that H has two left cosets (and thus two right cosets), that is $[G : H] = 2$. Consider the two cases $g \in H$ and $g \notin H$ and show that in both cases $gH = Hg$, that is H is normal in G.

2. Consider the dihedral group $D_n = \{r^i s^j,\ r^n = s^2 = (rs)^2 = 1\}$. Prove or disprove that $D_6 \simeq D_3 \times C_2$ where C_2 is the cyclic group with 2 elements (you may want to use 1.).

Answer.

1. If $g \in H$, then $gH = H = Hg$. Now if $g \notin H$, then gH cannot intersect with H (cosets are either disjoint or the same), but since we have only two cosets, both of them of size $|H|$ (and thus $|G| = 2|H|$), we have that gH must be everything in G which is not in H: $G \backslash H$. But the same is true for the right coset Hg, and so $gH = Hg$.

2. Let us first see if we can find a copy of D_3 inside D_6. In order to compute in D_6, we need to remember that:

   $$rsrs = 1 \iff rsr = s \iff rs = sr^{-1} \Rightarrow r^2 s = rsr^{-1} = sr^{-2} \Rightarrow r^i s = sr^{-i}$$

   for any i. To have D_3, we need rotations by $(2\pi/3)l$, $l = 0, 1, 2$, so they are found by considering the rotations r^{2l}, $l = 0, 1, 2$. We thus have that $(r^{2l})^3 = 1$ and $(r^2 s)^2 = r^2 s r^2 s = 1$ and $D_3 \simeq \{r^{2l} s^k, r^3 = s^2 = (rs)^2 = 1\}$. We need to see whether the two subgroups $H \simeq D_3$ and $K \simeq C_2$ are normal and such that $D_6 = HK$ and $H \cap K = \{1\}$. For D_3, it is normal because of 1., while for C_2 we still need to identify which subgroup this is, and whether it is normal. We know that we will need $H \cap K = \{1\}$ to be true, so we look for a subgroup of order 2 which does not intersect the one we have. Rotations r, r^3, r^5 are good candidates since they do not intersect with $r^{2l} s^k$, so we choose the one of order 2, that is $C_2 \simeq \langle r^3 \rangle$. It is a normal subgroup since for $j = 1$,

   $$r^i s^j (r^3) s^{-j} r^{-i} = r^i s (r^3 s) r^{-i} = r^i s (s r^{-3}) r^{-i} = r^{-3}$$

   and for $j = 0$, we have $r^i r^3 r^{-i}$. So we have found two normal subgroups $H \simeq D_3$ and $K \simeq C_2$, their intersection is trivial, and since $HK = \{r^{2l} s^k\} \cup \{r^{2l} s^k r^3\} = \{r^{2l} s^k\} \cup \{r^{2l} r^{-3} s^k\}$ (with the same powers and relations as above), we see that $HK = D_6$ and the isomorphism is true.

2.6 Group action

Exercise 26. 1. Let $G = GL_n(\mathbb{C})$ and $X = \mathbb{C}^n - \{\mathbf{0}\}$. Show that G acts on X by $G \times X \to X$, $(M, \nu) \mapsto M\nu$.

2. Show that the action is transitive.

Answer.

1. We have to show that

   $$M \cdot (M' \cdot \nu) = (MM') \cdot \nu,\ 1_G \cdot \nu = \nu.$$

   The first point is clear by properties of matrix vector multiplication. The second is also clear since 1_G is the identity matrix.

2. We have to show that there is only one orbit (which is why we have to remove the whole zero vector from $\mathbb{C}^n$). For that, we need to show that for any two vectors $\nu, \nu' \in X$, there is a matrix $M \in G$ such that $M\nu = \nu'$. We thus have a system of n linear equations for n^2 unknowns, so that we have enough degrees of freedom to find such a matrix. Alternatively, if $\nu = (a_1, \ldots, a_n)$, $\nu' = (b_1, \ldots, b_n)$, where a_i, b_i are all non-zero, take the matrix
$$\mathrm{diag}(a_1^{-1}, \ldots, a_n^{-1})$$
and notice that
$$\mathrm{diag}(b_1, \ldots, b_n)\mathrm{diag}(a_1^{-1}, \ldots, a_n^{-1})\nu = \nu'.$$
The case where some a_i, b_j are zero can be done similarly.

Exercise 27. Let G be group, and H be a subgroup of G. Show that
$$g \cdot g'H = gg'H$$
defines an action of G on the set G/H of cosets of H. Find the stabilizer of gH.

Answer. To show that the action is well defined we have to check that it does not depend on the choice of the representative, and that it satisfies the definition of group action. First suppose that $g'H = g''H$. We have to show that $g \cdot g''H = gg'H$. But $g'H = g''H \iff (g'')^{-1}g' \in H \iff (gg'')^{-1}(gg') \in H \iff gg'H = gg''H$. The definition of group action can be checked easily:
$$g_1 \cdot (g_2 \cdot g'H) = g_1 \cdot g_2g'H = g_1g_2g'H = g_1g_2 \cdot g'H,\ 1 \cdot g'H = g'H.$$
The stabilizer of gH is formed by g' such that $g'gH = gH$ that is $g^{-1}g'g \in H$. Thus $g^{-1}g'g = h$, for some $h \in H$, or equivalently $g' = ghg^{-1}$, thus the stabilizer is gHg^{-1}.

Exercise 28. Consider the *dihedral group* D_8 given by
$$D_8 = \{1, s, r, r^2, r^3, rs, r^2s, r^3s\}$$
(that is $s^2 = 1$, $r^4 = 1$ and $(rs)^2 = 1$).

1. Divide the elements of the dihedral group D_8 into conjugacy classes.
2. Verify the class equation.

Answer.

1. There are 5 conjugacy classes
$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}.$$
2. We have that $\{1\}$ and $\{r^2\}$ are in the center. Thus
$$|D_4| = 8 = |Z(D_4)| + |\mathrm{Orb}(r)| + |\mathrm{Orb}(rs)| + |\mathrm{Orb}(s)|.$$

Exercise 29. The *quaternion group* Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{aligned} 1 \cdot a = a \cdot 1 = a, \ \forall\ a \in Q_8 \\ (-1) \cdot (-1) = 1, \ (-1) \cdot a = a \cdot (-1) = -a, \ \forall\ a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 \\ i \cdot j = k, \ j \cdot i = -k, \\ j \cdot k = i, \ k \cdot j = -i, \\ k \cdot i = j, \ i \cdot k = -j. \end{aligned}$$

1. Show that if $x \notin Z(Q_8)$, then $|C_{Q_8}(x)| = 4$.
2. Show that as a consequence, the class of conjugacy of $x \notin Z(D_8)$ has only two elements.

Answer.

1. The center $Z(Q_8)$ is $Z(Q_8) = \{1, -1\}$. We have by definition that

   $$C_{Q_8}(x) = \{g \in Q_8, \ gx = xg\}.$$

   Thus

   $$C_{Q_8}(i) = \{1, -1, i, -i\},\ C_{Q_8}(j) = \{1, -1, j, -j\},\ C_{Q_8}(k) = \{1, -1, k, -k\}.$$

2. When the action is defined by conjugation, we have that $\mathrm{Stab}(x) = C_{Q_8}(x)$. Thus by the Orbit-Stabilizer, the size of an orbit, which is a conjugacy class, is

   $$|B(x)| = |Q_8|/|C_{Q_8}(x)| = 8/4 = 2.$$

Exercise 30. Let G be a group and let H and K be two subgroups of G.

1. Show that the subgroup H acts on the set of left cosets of K by multiplication.
2. Consider the coset $1K = K$. Compute its orbit $B(K)$ and its stabilizer $\mathrm{Stab}(K)$.
3. Compute the union of the cosets in $B(K)$ and deduce how many cosets are in the orbit.
4. Use the Orbit-Stabilizer Theorem to get another way of counting the number of cosets in $B(K)$. By comparing the two expressions to count the cardinality of $B(K)$, find a formula for the cardinality of HK.

Answer.

1. Let $X = \{gK,\ g \in G\}$ be the set of left cosets of K. We have to check that $h' \cdot (h \cdot gK) = (h'h) \cdot gK$ which clearly holds, as does $1_H \cdot gK = gK$.

2. We have that $B(K) = \{h \cdot K,\ h \in H\}$ and $\text{Stab}(K) = \{h \in H,\ h \cdot K = K\} = H \cap K$.

3. The union of the cosets in $B(K)$ is HK, the cosets in $B(K)$ are disjoint and each has cardinality K, so that we have $|HK|/|K|$ cosets in $B(K)$.

4. By the Orbit-Stabilizer Theorem, we have

$$|B(K)| = |H|/|\text{Stab}(K)| \Rightarrow |HK|/|K| = |H|/|H \cap K|$$

and thus

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

Exercise 31. Let G be a finite group, and let p be the smallest prime divisor of the order of G.

1. Let H be a normal subgroup of G. Show that G acts on H by conjugation.

2. Let H be a normal subgroup of G of order p.

   - Show that the orbits of H under the action of G are all of size 1.
   - Conclude that a normal subgroup H of order p is contained in the center of G.

Answer.

1. We check the definition, that is, the group G acts on H if for the map $(g, x) \mapsto g \cdot x = gxg^{-1}$, $x \in H$, defined from $G \times H \to H$ (note that we need here H normal to guarantee that $gxg^{-1} \in H$!), we have

   - $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = h(gxg^{-1})h^{-1} = (hg) \cdot x$
   - $1 \cdot x = x$ for all $x \in H$

2. - By the orbit stabilizer theorem, the size of an orbit $B(x), x \in H$ divides the size of G, the group that acts on H, thus if $|B(x)|$ is not 1, it must be at least p, since p is the smallest divisor of the order of G. Now the orbits partition H, that is $H = \cup B(x)$ and thus $|H| = \sum |B(x)|$, that is the sum of the cardinals of the orbits is $|H| = p$. Among all the $B(x)$, we can take $x = 1 \in H$ since H is a subgroup. The orbit $B(1) = \{g \cdot 1, g \in G\} = \{g1g^{-1} = 1\}$ has only 1 element, there is at least one orbit of size 1, and thus no orbit can have size greater or equal to p, since then $p + 1 > p$. Thus all orbits of H are of size 1.

- We have that $B(x) = \{g \cdot x, g \in G\} = \{gxg^{-1}, g \in G\}$ is always of size 1, and since for $g = 1 \in G$ we have $x \in B(x)$, we deduce that $B(x) = \{x\}$, that is $gxg^{-1} = x$, or $gx = xg$ showing that for all $x \in H$, x actually commutes with every $g \in G$, that is, H is contained in the center.

Exercise 32. Let G be a group acting on a finite set X.

1. We assume that every orbit contains at least 2 elements, that $|G| = 15$, and that $|X| = 17$. Find the number of orbits and the cardinality of each of them.

2. We assume that $|G| = 33$ and $|X| = 19$. Show that there exists at least one orbit containing only 1 element.

Answer.

1. The cardinal of every orbit divides the order of G. Furthermore, the sum of the orbit cardinalities is equal to the cardinality of X. If $|G| = 15$, $|X| = 17$, and there is no orbit of size 1, there is only one possibility: 4 orbits of length 3 and 1 of length 5. Indeed, we are looking for integers such that their sum is 17, but each integer must divide 15, that is we need to realize 17 as a sum of integers belonging to $\{3, 5, 15\}$ (1 is excluded by assumption). Then 15 is not possible, and we can use only 3 and 5: 15+2 is not possible, 10+7 is not possible, so only 5+12 works.

2. Now $|G| = 33$ and $|X| = 19$. The divisors of 33 are 1,3,11 and 33. We need to obtain as above 19 as a sum of these divisors. 33 is too big, and we cannot possibly use only 11 and 3. Thus there must be at least one orbit of size 1.

Exercise 33. (**) Let G be a finite group of order $n \geq 1$ and let p be a prime. Consider the set

$$X = \{x = (g_1, g_2, \ldots, g_p) \ \in G^p \mid g_1 \cdot g_2 \cdots g_p = 1_G\}.$$

1. Compute the cardinality $|X|$ of the set X.

2. Show that if $(g_1, \ldots, g_p) \in X$, then $(g_2, \ldots, g_p, g_1) \in X$. Denote by σ the corresponding permutation. Show that $< \sigma >$ acts on X as follows:

$$\sigma^k \cdot (g_1, \ldots, g_p) = (g_{\sigma^k(1)}, \ldots, g_{\sigma^k(p)}), \ k \in \mathbb{Z}$$

3. What is the cardinal of one orbit of X?

4. What are the orbits with one element? Show that there is at least one such orbit.

5. Deduce that if p does not divide n, then

$$n^{p-1} \equiv 1 \mod p.$$

6. Deduce Cauchy Theorem from the above, namely, if $p \mid n$ then G has at least one element of order p.

Answer.

1. Since $g_1, \ldots, g_{p-1}$ can take any value in G (only g_p is constrained so as to have $g_1 \cdot g_2 \cdots g_p = 1_G$), we have $|X| = |G|^{p-1} = n^{p-1}$.

2. Since $(g_1, \ldots, g_p) \in X$, then $g_1 \cdot g_2 \cdots g_p = 1_G$ and $g_2 \cdots g_p \cdot g_1 = g_1^{-1} \cdot 1_G \cdot g_1$ showing that $(g_2, \ldots, g_p, g_1) \in X$. To show that $< \sigma >$ acts on X, check the definition, namely $\sigma^l \cdot (\sigma^k \cdot (g_1, \ldots, g_p)) = \sigma^l \sigma^k \cdot (g_1, \ldots, g_p)$ and $\sigma^0 \cdot (g_1, \ldots, g_p) = (g_1, \ldots, g_p)$.

3. The answer is either 1 or p. There are two ways to do it: one can notice that $< \sigma >$ has order p, and thus by the Orbit-Stabilizer Theorem the size of the orbit divides p, so it can be either 1 or p. Also one can just write down the definition of one orbit: the orbit of $(g_1, \ldots, g_p)$ is formed by all the shifts of the components, and thus since p is prime, there will be p distinct shifts, apart if all the components are all the same, in which case there is only one element in the orbit.

4. Since an element always belongs to its orbit, we have that orbits with one element are of the form $B(x) = \{x\}$, and if there is only one element, that means that the shifts are doing nothing on $x = (g_1, \ldots, g_p)$ thus $x = (g, \ldots, g)$ and since $x \in X$, that further means that $g^p = 1_G$. To show one such orbit exists, take the orbit of $(1, \ldots, 1)$.

5. Since the orbits partition X, we have

$$|X| = \sum |B(x)| + \sum |B(x')|$$

where the first sum is over orbits of size 1, and the second over orbits of size greater or equal to 2. By the above, if the size is at least 2, it is p, and thus $|B(x')| \equiv 0 \mod p$. Then if there were more than $(1, \ldots, 1)$ with orbit of size 1, that means an element g such that $g^p = 1$, which would mean $p|n$, a contradiction. Thus only there is only one orbit of size 1, and

$$|X| = n^{p-1} \equiv 1 \mod p.$$

6. Again, we have that

$$n^{p-1} = |X| = \sum |B(x)| + \sum |B(x')|$$

and if $p|n$ then $0 \equiv \sum |B(x)|$ and there must be at least another element with orbit size 1, that is an element g of order p.

2.7 Classification of Abelian groups

Exercise 34. Let $\phi : G \to H$ be a group homomorphism, for G, H two groups.

1. Prove that the order of $\phi(g)$ divides the order of g.
2. Prove that if ϕ is injective, then the order of $\phi(g)$ is equal to that of g.
3. For N a normal subgroup of G, show that $|gN|||g|$.

Answer.

1. Suppose g has order n. Then $g^n = 1$, thus $\phi(g^n) = \phi(g)^n = \phi(1) = 1$. This shows that $\phi(g)^n = 1$ so either $\phi(g)$ has order n, or its order is some m smaller than n. Suppose there is such m, then $\phi(g)^m = 1$ and m is then the smallest positive integer with this property. Divide n by m to find $n = mq + r$ with $r < m$, then
$$1 = g^n = g^{mq+r} = (g^m)^q g^r = g^r$$
thus $r = 0$ and m divides n as needed.
2. Say $\phi(g)$ has order m. Then $\phi(1) = 1 = \phi(g)^m = \phi(g^m)$ and since ϕ is injective, we must have $g^m = 1$, which shows that $m = n$.
3. Choose for ϕ the canonical map $\phi : G \to G/N$. Then $\phi(g) = gN$ and apply 1.

Exercise 35. List all the abelian groups of order 36.

Answer. Write $36 = 2^2 \cdot 3^2$. Then 2^2 can give rise to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Similarly, 3^2 can give rise to either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$. This thus gives 4 cases:

1. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/36\mathbb{Z}$,
2. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$,
4. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Exercise 36. Decide whether the following groups are isomorphic:

- $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
- $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
- $\mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$.

Answer.

- $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, this is because $\mathbb{Z}/4\mathbb{Z}$ is a cyclic group (under addition), while $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not, it is isomorphic to the Klein group. It can be easily checked there is no element of order 4, and all elements but the identity $(0, 0)$ have order 2.

- $\mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, both of them are cyclic of order 6. To see this, it is enough to see that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ contains an element of order 6, namely $(1, 1)$.

- $\mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$. We apply the classification of abelian groups to decompose $\mathbb{Z}/48\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/54\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, therefore

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \not\simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}.$$

  Note for example that $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/16\mathbb{Z}$. The reason is illustrated in the first two parts of the exercise. When m, n are coprime then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$, this is because $(1, 1)$ will have order mn, which is not the case when m, n are not coprime.