7. Groups

We begin with a series of definitions:

Definition 7.1. Let G be a set. A *(binary) operation* or a *composition law* $*$ in G is a map:

$$*\colon G \times G \to G.$$

Instead of writing $*(a, b)$ to indicate the result of applying the map $*$ to the pair $(a, b) \in G \times G$, we will usually write $a * b$.

Definition 7.2. An operation $*$ on G is called *associative* if and only if

$$(a * b) * c \;=\; a * (b * c) \quad \text{for all} \quad a, b, c \in G. \tag{7.1}$$

Definition 7.3. An operation $*$ on G is called *commutative* if and only if

$$a * b \;=\; b * a \quad \text{for all} \quad a, b \in G. \tag{7.2}$$

Definition 7.4. Given a set G with a binary operation $*$, an element $e \in G$ is called an identity element for $*$ if and only if:

$$a * e \;=\; e * a \;=\; a \quad \text{for all} \quad a \in G. \tag{7.3}$$

Even though, in principle, a set G with a binary operation $*$ could have different identity elements, it is easy to prove that, in fact, if an identity element exists then it must be unique:

Proposition 7.5. *Let G be a set with a binary operation $*$. Then if an identity element exists it is unique.*

Proof. Suppose e_1 and e_2 are elements in G satisfying (7.3). Then we have

$$e_2 = e_1 * e_2 = e_1,$$

where in the first equality we use the fact that e_1 is an identity and in the second equality that e_2 is an identity. □

Definition 7.6. Given a set G with a binary operation $*$ and an identity element e, we say that $b \in G$ is an inverse of $a \in G$ if and only if

$$a * b \;=\; b * a \;=\; e \tag{7.4}$$

Once again, it is easy to prove that, for associative operations, if an inverse exists then it must be unique:

Proposition 7.7. *Let G be a set with a binary operation $*$ and suppose there exists an identity e. Then if an inverse of an element a exists, it is unique.*

Proof. Suppose b and c are inverses of a. Then we have:

$$\begin{aligned} b &= b * e && \text{(since } e \text{ is the identity)} \\ &= b * (a * c) && \text{(since } c \text{ is an inverse of } a) \\ &= (b * a) * c && \text{(by associativity)} \\ &= e * c && \text{(since } b \text{ is an inverse of } a) \\ &= c && \text{(since } e \text{ is the identity)} \end{aligned}$$

□

Definition 7.8. A *group* is a set G with an operation $*$ such that:

i) $*$ is associative.
ii) There exists an identity element $e \in G$.
iii) Every element $a \in G$ has an inverse.

If, in addition, $*$ is commutative then we say that G is a *commutative* group or an *abelian* group.

Example 7.9. The integers $\mathbb{Z}$ with $* = +$ is an abelian group. We know that addition is associative and commutative and 0 is the identity element. Moreover, given any $a \in \mathbb{Z}$, $-a$ is the inverse of a.

Exactly the same arguments show that the rational numbers $\mathbb{Q}$ or the real numbers $\mathbb{R}$ with the operation of addition are abelian groups whose identity element is 0.

Example 7.10. Consider now the same set $\mathbb{Z}$ but with the operation $* =$ product. We know that the product of integers is associative and commutative. Moreover, the element 1 is the identity element since $1 \cdot m = m \cdot 1 = m$ for all $m \in \mathbb{Z}$. However, it is not true that every element has an inverse. In fact, the only elements with an inverse are 1 and -1. So, $\mathbb{Z}$ with the multiplication operation **is not** a group.

Consider next the set $\mathbb{Q}$ with the multiplication operation. Again, the product of rational numbers is associative, commutative and 1 is the identity element. What about existence of inverse? Every element except 0 has an inverse: if $a = p/q$ and $p, q \neq 0$ then $b = q/p$ is the inverse of a. But the element 0 does not have an inverse: We cannot find a rational number b such that $0 \cdot b = 1$!

Since 0 is the only element without an inverse and the product of non-zero numbers is not zero we can restrict the product operation to the set

$$\mathbb{Q}^* := \{a \in \mathbb{Q} : a \neq 0\}$$

to get an abelian group. Similarly, we can define a multiplicative group $(\mathbb{R}^*, \cdot)$, where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Example 7.11. Note that there is no a priori restriction on what an operation is, just that it is a map that to each ordered pair of elements of G assigns

another element of G. For example G could be the set $G = \{p, s, r\}$ and the operation be:

$$p * p = p \ ; \quad s * s = s \ ; \quad r * r = r \ ;$$

$$p * s = s * p = s \ ; \quad p * r = r * p = p \ ; \quad r * s = s * r = r.$$

(This is the operation derived from the paper/scissors/rock game.) Note that in this case the operation is commutative by definition. However, we see by inspection that there is no identity element. Is it associative? We have:

$$(p * s) * r = s * r = r,$$

but

$$p * (s * r) = p * r = p.$$

So, $*$ is not associative.

The following is one of the key examples and the one from which the term *composition law* is derived.

Example 7.12. Let X be an arbitrary non-empty set and let

$$\mathcal{B}(X) \ := \ \{f \colon X \to X : f \text{ is bijective } \},$$

and set $f * g = f \circ g$, the composition of maps. This makes sense since the composition of bijections is a bijection. We have already shown that the composition of maps is associative and that the identity map id_X satisfies that

$$f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f.$$

Therefore, id_X is the identity for $(\mathcal{B}(X), *)$.

Moreover, we have also proved that every bijection $f \in \mathcal{B}(X)$ has an inverse map $f^{-1} \in \mathcal{B}(X)$ satisfying:

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X.$$

Thus, the inverse in the sense of maps is also the inverse for $*$. Therefore $(\mathcal{B}(X), *)$ is a group. Note that in general this group is not commutative. For example if

$$X = \{1, \ldots, n\}$$

then $\mathcal{B}(X)$ is the set of permutations of $\{1, \ldots, n\}$ and we have already seen that the composition of permutations is not commutative. Recall that in this case we denote by S_n the group of permutations of $\{1, \ldots, n\}$.

8. The integers mod m. Modular Arithmetic.

In this section we will study in detail operations defined in a space of equivalence classes. This is the most important example of a group that we will study in this course.

We begin by recalling that given an integer $m > 1$, we have defined an equivalence relation on $\mathbb{Z}$:

$$a \sim b \Leftrightarrow m|(a-b).$$

Since we will be studying this particular equivalence relation in detail we introduce a specific notation to replace the generic notation $\sim$. We will say that:

$$a \equiv b \pmod{m} \;\Leftrightarrow\; m|(a-b)$$

Let $R_m \colon \mathbb{Z} \to \{0, 1, \ldots, m-1\}$ be the map that assigns to each $a \in \mathbb{Z}$ the remainder of dividing a by m; i.e. $R_m(a)$ is the unique integer between 0 and $m-1$ such that there exists $k \in \mathbb{Z}$ with

$$a \;=\; k \cdot m + R_m(a).$$

(**What theorem guarantees the existence and uniqueness of this decomposition?**)

Then, since $m|(a-b)$ if and only if $R_m(a) = R_m(b)$ we have that

$$a \equiv b \pmod{m} \;\Leftrightarrow\; R_m(a) = R_m(b).$$

This means that the map R_m defines the equivalence relation $a \equiv b \pmod{m}$ and, consequently, the quotient space of this equivalence relation $\mathbb{Z}/\sim$ is bijectively equivalent to $\{0, 1, \ldots, m-1\}$. To keep track of the integer m used to define the equivalent relation we will denote $\mathbb{Z}/\sim$ by $\mathbb{Z}_m$.

We now define an operation $\oplus$ in the set $\mathbb{Z}/\sim$ of equivalence classes in the following way: Let C_1 and C_2 be equivalence classes, pick $a_1 \in C_1$ and $a_2 \in C_2$ then define:

$$C_1 \oplus C_2 \;:=\; [a_1 + a_2] \tag{8.1}$$

Before we can accept this as a valid definition we need to check that the result of the operation does not depend on our pick of representatives a_1 and a_2 in the equivalence classes C_1 and C_2. Suppose we pick different elements, say $b_1 \in C_1$ and $b_2 \in C_2$, then

$$a_1 \equiv b_1 \pmod{m} \;\Rightarrow\; m|(a_1 - b_1), \quad \text{and}$$

$$a_2 \equiv b_2 \pmod{m} \;\Rightarrow\; m|(a_2 - b_2)$$

But then m divides $(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$. Therefore

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

and $[a_1 + a_2] = [b_1 + b_2]$.

For example, let $m = 4$, then there are 4 equivalence classes in $\mathbb{Z}_4$ which we can list as $[0], [1], [2], [3]$ and we have the following table for $\oplus$

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Remark: Since the set $\mathbb{Z}/\sim = \mathbb{Z}_m$ is bijectively equivalent to the set $\{0, 1, \ldots, m-1\}$ we may think of $\oplus$ as an operation on the set $\{0, 1, \ldots, m-1\}$. With this point of view, the table above describes an operation in the set $\{0, 1, 2, 3\}$. Once one is used to the notion of quotients it is common to forget the square brackets and to replace the symbol $\oplus$ by the standard $+$. But, for the remaining of these notes we will keep the clumsier notation so we can be sure of where we are working.

We now check the conditions for $(\mathbb{Z}_m, \oplus)$ to be a group:

Associativity:

$$([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c] = [a] + ([b] + [c]).$$

Identity: The class $[0]$ is the identity element since:

$$[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a].$$

Existence of Inverse: For each $[a] \in \mathbb{Z}_m$ the element $[-a]$ is the inverse of $[a]$ since:

$$[a] + [-a] = [a - a] = [0] = [-a + a] = [-a] + [a].$$

Hence, $(\mathbb{Z}_m, \oplus)$ is a group. In fact, it is equally easy to check that $(\mathbb{Z}_m, \oplus)$ is an abelian group. We leave the verification to the reader.

Remark: We make an important notational comment. When operating in $\mathbb{Z}_m$ the expressions:

$$a + b \equiv c \pmod{m}$$

and

$$[a] \oplus [b] = [c]$$

are completely equivalent. Notice that the first expression conveys more information since it makes explicit what m is. The second expression is simpler once m is fixed. For example the statements

$$5 + 11 \equiv 2 \pmod{7}$$

is equivalent to saying: In the group $\mathbb{Z}_7$

$$[5] \oplus [11] = [2].$$

But note that for the second expression to make sense we need to specify the group where the operation takes place.

We can similarly define a multiplication $\otimes$ in the set $\mathbb{Z}/\sim = \mathbb{Z}_m$ as follows: Let C_1 and C_2 be equivalence classes, pick $a_1 \in C_1$ and $a_2 \in C_2$ then define:

$$C_1 \oplus C_2 \ := \ [a_1 \cdot a_2] \tag{8.2}$$

Once again we need to check that this definition does not depend on the representatives a_1 and a_2 that we picked.

Suppose we pick different elements, say $b_1 \in C_1$ and $b_2 \in C_2$, then since $a_1 \equiv b_1 \pmod{m}$ we have from the Division Theorem that:

$$a_1 = k_1 m + r_1 \ ; \quad b_1 = \ell_1 m + r_1 \ ; \quad 0 \leq r_1 < m.$$

(**Why are the remainders the same?**)

Similarly,

$$a_2 = k_2 m + r_2 \ ; \quad b_2 = \ell_2 m + r_2 \ ; \quad 0 \leq r_2 < m.$$

We then have:

$$a_1 \cdot a_2 = k_1 k_2 m + k_1 r_2 m + k_2 r_1 m + r_1 r_2 \equiv r_1 \cdot r_2 \pmod{m},$$

$$b_1 \cdot b_2 = \ell_1 \ell_2 m + \ell_1 r_2 m + \ell_2 r_1 m + r_1 r_2 \equiv r_1 \cdot r_2 \pmod{m}.$$

Which means that $[a_1 \cdot a_2] = [b_1 \cdot b_2]$. So, the *modular product* $\otimes$ is well defined.

Example 8.1. Let us write the table for the modular product in $\mathbb{Z}_4$.

$\otimes$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Just as we did in the case of $\oplus$ we can easily check that $\otimes$ is associative, commutative, and that [1] is the identity element. However, we cannot expect to have an inverse since the element [0] will never have an inverse. We already encountered this problem in the example of the product operation in $\mathbb{Q}$ and we solved it by considering the set $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Can we do the same thing here? The table for $\mathbb{Z}_4$ tells us that the answer is NO since the element [2] has no inverse either!! It is then natural to ask:

Question: When does an element $[a] \in \mathbb{Z}_m$ have an inverse in $\mathbb{Z}_m$; i.e. when can we find $b \in \mathbb{Z}$ so that $[a] \otimes [b] = [1]$?

Fortunately, the answer to this question is very easy:

Theorem 8.2. *Let $[a] \in \mathbb{Z}_m$ then $[a]$ has an inverse in $(\mathbb{Z}_m, \otimes)$ if and only if $\gcd(a, m) = 1$.*

Proof. Suppose that $[a]$ has an inverse $[b]$, then $[a] \otimes [b] = [1]$; i.e.

$$a \cdot b \equiv 1 \pmod{m}$$

and this means that there exists $k \in \mathbb{Z}$ such that

$$a \cdot b = k \cdot m + 1.$$

But then

$$1 = a \cdot b - k \cdot m$$

and it follows that $\gcd(a, m) = 1$. The converse is identical: if $\gcd(a, m) = 1$ then there exist integers x, y such that

$$1 = a \cdot x + m \cdot y$$

But this implies that

$$a \cdot x \equiv 1 \pmod{m}$$

or, equivalently, that $[a] \otimes [x] = [1]$ and $[x]$ is the inverse of $[a]$ in $(\mathbb{Z}_m, \otimes)$. □

We can illustrate Theorem 8.2 in the case of $\mathbb{Z}_4$. The elements [1] and [3] have inverses since

$$\gcd(1, 4) = \gcd(3, 4) = 1.$$

But the elements [0] and [2] do not since

$$\gcd(0, 4) = 4 \quad \text{and} \quad \gcd(2, 4) = 2.$$

We have the following important Corollary to Theorem 8.2:

Corollary 8.3. *If p is prime then every non-zero element in $(\mathbb{Z}_p, \otimes)$ has an inverse. Therefore if we denote by $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$, then $(\mathbb{Z}_p^*, \otimes)$ is an abelian group.*

Proof. Let $[a] \in \mathbb{Z}_p$ and suppose that $[a] \neq [0]$. Then, p does not divide a and since p is prime we must have $\gcd(a, p) = 1$. Then by the Theorem, $[a]$ has an inverse in $\mathbb{Z}_p$. □

Example 8.4. Consider the multiplication table for $\mathbb{Z}_5$:

$\otimes$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

We see that in this case $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, and $[4]^{-1} = [4]$.

The fact that for a prime number p the operations in $\mathbb{Z}_p$, $\oplus$ and $\otimes$, satisfy the same properties as the addition and product of rational or real numbers[¶] means that we can operate with them just as we do with rationals or reals. Let's illustrate this point with a few examples.

Example 8.5. Solve the congruence equation

$$2x + 3 \equiv 4 \pmod 5.$$

We can view this expression as an equation in $\mathbb{Z}_5$:

$$([2] \otimes x) \oplus [3] = [4].$$

We then have

$$[2] \otimes x = [4] \oplus (-[3]) = [1] \quad \text{(here } - \text{ denotes the additive inverse in } (\mathbb{Z}_5, \oplus).)$$

Therefore

$$x = [2]^{-1} \otimes ([2] \otimes x) = [2]^{-1} \otimes [1] = [3]$$

since $[2]^{-1} = [3]$ in $\mathbb{Z}_5$ (see Example 8.4). We can verify our result:

$$2 \cdot 3 + 3 = 9 \equiv 4 \pmod 5.$$

Example 8.6. Now let us try something harder. Solve the congruence equation

$$15x + 11 \equiv 7 \pmod{31}.$$

We can view this expression as an equation in $\mathbb{Z}_{31}$:

$$([15] \otimes x) \oplus [11] = [7].$$

We then have

$$[15] \otimes x = [7] \oplus (-[11]) = [7] \oplus [20] = [27] \quad \text{(here } - \text{ denotes the inverse in } (\mathbb{Z}_5, \oplus).)$$

Therefore

$$x = [15]^{-1} \otimes ([15] \otimes x) = [15]^{-1} \otimes [27].$$

We now need to compute $[15]^{-1}$ in $\mathbb{Z}_{31}$. The proof of Theorem 8.2 tells us how to proceed: Since $\gcd(15, 31) = 1$ we can write 1 as an integral linear combination of 15 and 31. In this case this is very easy

$$1 = 31 + (-2) \cdot 15.$$

[¶]In addition to the properties we have already discussed, the modular product is distributive with respect to modular addition, that is:

$$[a] \otimes ([b] \oplus [c]) = ([a] \otimes [b]) \oplus ([a] \otimes [c])$$

as is easily verified from the definitions. It is also easy to check that $[a] \otimes [0] = [0]$ for all $[a] \in \mathbb{Z}_p$. All of these properties together define the notion of a *field*. The reals $\mathbb{R}$ and the rationals $\mathbb{Q}$ are fields as is $\mathbb{Z}_p$ for p prime. One big difference between them is that $\mathbb{Z}_p$ is finite, $\mathbb{Q}$ is denumerable, and $\mathbb{R}$ is uncountable.

This means that $(-2)\cdot 5 \equiv 1 \pmod{31}$, in other words that $[-2]\otimes[15] = [1]$ in $\mathbb{Z}_{31}$. So $[15]^{-1} = [-2]$ and $x = [-2]\otimes[27] = [-54] = [8]$. Again, it is worthwhile to verify our result:

$$15\cdot 8 + 11 = 131 = 4\cdot 31 + 7 \equiv 7 \pmod{31}.$$

Example 8.7. In this example we will use modular arithmetic to find the test for divisibility by 11. Let $m \in \mathbb{Z}_{>0}$ be a positive integer and write m in its decimal expansion:

$$m = a_k a_{k-1}\cdots a_1 a_0,$$

where a_j are digits between 0 and 9 and $a_k \neq 0$. In other words,

$$m = a_k\cdot 10^k + a_{k-1}\cdot 10^{k-1} + \cdots + a_1\cdot 10 + a_0.$$

Theorem 8.8. *m is divisible by 11 if and only if the alternating sum*

$$a_0 - a_1 + a_2 + \cdots + (-1)^k a_k \;=\; \sum_{j=0}^{k}(-1)^j a_j$$

is divisible by 11.

Proof. We will work in $\mathbb{Z}_{11}$. If m is divisible by 11 then $[m] = [0]$ in $\mathbb{Z}_{11}$ and therefore we have

$$[a_k]\otimes[10^k]\oplus[a_{k-1}]\otimes[10^{k-1}]\oplus\cdots\oplus[a_1]\otimes[10]\oplus[a_0] = [0].$$

But $[10] = [-1]$ in $\mathbb{Z}_{11}$, therefore the above expression may be rewritten as

$$[a_k]\otimes[(-1)^k]\oplus[a_{k-1}]\otimes[(-1)^{k-1}]\oplus\cdots\oplus[a_1]\otimes[-1]\oplus[a_0] = [0],$$

or, given the definitions of $\otimes$ and $\oplus$ as:

$$(-1)^k\cdot a_k + (-1)^{k-1}\cdot a_{k-1} + \cdots - a_1 + a_0] = [0]$$

which means that

$$a_0 - a_1 + a_2 + \cdots + (-1)^k a_k$$

is divisible by 11. □

So, for example, 385 is divisible by 11 since the alternating sum of the coefficients is $5 - 8 + 3 = 0$ and 0 is divisible by 11. But 749 is not divisible by 11 since, in this case, the alternating sum is: $9 - 4 + 7 = 12$ which is not divisible by 11.

9. Subgroups - Cyclic Groups

Definition 9.1. Let $(G, *)$ be a group. A non-empty subset $H \subseteq G$ is called a subgroup if and only if

i) If $h_1, h_2 \in H$ then $h_1 * h_2 \in H$.
ii) For every $h \in H$, the inverse $h^{-1} \in H$.

Remark: If $H \subseteq G$ is a subgroup of $(G, *)$ then $(H, *)$ is a group as well. We only need to check that H has an identity element but this is implied by i) and ii) in Definition 9.1. Indeed, pick any element $h \in H$ (we required H to be non-empty), then by ii), $h^{-1} \in H$ and by i), $e = h^{-1} * h \in H$. But then e is also the identity element in H.

Example 9.2. The integers $\mathbb{Z}$ are a subgroup of $(\mathbb{Q}, +)$. Indeed, if $m, n \in \mathbb{Z}$ then $m + n \in \mathbb{Z}$ and $-m \in \mathbb{Z}$. On the other hand, $\mathbb{Z}_{>0}$ is not a subgroup of $\mathbb{Z}$. While it is true that for $m, n \in \mathbb{Z}_{>0}$, $m + n \in \mathbb{Z}_{>0}$, it is not true that for $m \in \mathbb{Z}_{>0}$, $-m \in \mathbb{Z}_{>0}$. Therefore the second condition in Definition 9.1 fails.

Example 9.3. For any $n \in \mathbb{Z}_{>0}$,

$$n\mathbb{Z} := \{k \in \mathbb{Z} : n|k\}$$

is a subgroup of $(\mathbb{Z}, +)$. Indeed, if n divides k_1 and k_2 then n divides $k_1 + k_2$ and if n divides k then n divides $-k$. Therefore both conditions in Definition 9.1 are satisfied.

Example 9.4. Consider the group $(\mathbb{Z}_4, \oplus)$. It follows from the operation table for this group that the subset $H = \{[0], [2]\}$ is a subgroup. Indeed, in $\mathbb{Z}_4$:

$$[0] \oplus [0] = [2] \oplus [2] = [0] \; ; \quad [0] \oplus [2] = [2] \oplus [0] = [2]$$

and $-[0] = [0]$ and $-[2] = [2]$, where as always, $-$ denotes the inverse in $(\mathbb{Z}_4, \oplus)$.

Given a group $(G, *)$ and an element $g \in G$ we may define the n-th power of g recursively:

- $g^1 = g$;
- Assuming we have defined g^n then we define $g^{n+1} = g^n * g$.

This defines g^n for every $n \in \mathbb{Z}_{>0}$. We also define: $g^0 = e$ and for $n \in \mathbb{Z}_{>0}$:

$$g^{-n} = (g^{-1})^n.$$

Note that g^{-1} is the inverse of g with respect to $*$.

The following Lemma will be useful in proving a very important Theorem.

Lemma 9.5. *For every $n \in \mathbb{Z}$,*

$$g^{-n} = (g^{-1})^n.$$

Proof. Note that the statement follows from the definition if $n > 0$ while it is obvious if $n = 0$. We need to consider then the case $n < 0$. But then

$$(g^{-1})^n = ((g^{-1})^{-1})^{-n} = g^{-n}.$$

□

Theorem 9.6. *Let $(G, *)$ be a group and let $g \in G$. Then for all $\ell, k \in \mathbb{Z}$:*

$$g^\ell * g^k = g^{\ell+k}.$$

Proof. This proof is a good example of an argument which appears to be obvious but that requires quite a bit of work in order to prove it with the ingredients at our disposal. The main difficulty is that we have different definitions for positive and negative powers.

We will fix $\ell \in \mathbb{Z}$ and prove the assertion of the Lemma for all $k \in \mathbb{Z}$.

We begin with the easiest case: $k = 0$, then

$$g^\ell * g^0 = g^\ell * e = g^\ell = g^{\ell+0}.$$

Next, we prove the result for $k \in \mathbb{Z}_{>0}$ by induction. We begin with the base case $k = 1$. We need to distinguish three cases depending on whether $\ell > 0$, $\ell = 0$, or $\ell < 0$.

i) If $\ell > 0$, then $g^\ell * g^1 = g^\ell * g = g^{\ell+1}$ by the recursive definition of the powers of an element.
ii) If $\ell = 0$, then $g^0 = e$ and $g^0 * g^1 = e * g^1 = g^1 = g^{0+1}$.
iii) Suppose now that $\ell < 0$, and write $\ell = -s$ with $s > 0$. Then $g^\ell = (g^{-1})^s = (g^{-1})^{s-1} * (g^{-1})$ by the previous cases (remember that $s \geq 0$). Then

$$\begin{aligned} g^\ell * g^1 &= ((g^{-1})^{s-1} * (g^{-1})) * g \\ &= (g^{-1})^{s-1} * ((g^{-1}) * g) \\ &= (g^{-1})^{s-1} * e = (g^{-1})^{s-1} \\ &= g^{-(s-1)} \\ &= g^{\ell+1} \end{aligned}$$

Suppose now that the $g^\ell * g^n = g^{\ell+n}$ for all all $\ell \in \mathbb{Z}$ and some $n \in \mathbb{Z}_{>0}$. We want to prove that

$$g^\ell * g^{n+1} = g^{\ell+n+1}.$$

Now, by definition $g^{n+1} = g^n * g$, therefore

$$\begin{aligned} g^\ell * g^{n+1} &= g^\ell * (g^n * g) && \\ &= (g^\ell * g^n) * g && \text{(associativity)} \\ &= g^{\ell+n} * g && \text{(inductive hypothesis)} \\ &= g^{\ell+n+1} && \text{(base case)} \end{aligned}$$

Unfortunately, our work is not yet done because we have only proved the assertion of the Lemma for $\ell \in \mathbb{Z}$ and $k \in \mathbb{Z}_{\geq 0}$. We still need to consider the case $k < 0$. However we can use a trick to reduce it to the case we have already proved! If $k < 0$, then $k = -r$ with $r > 0$ and $g^k = (g^{-1})^r$ by

definition. Moreover, by Lemma 9.5, we have $g^\ell = (g^{-1})^{-\ell}$. Then

$$\begin{aligned} g^\ell * g^k &= (g^{-1})^{-\ell} * (g^{-1})^r \\ &= (g^{-1})^{-\ell+r} \qquad \text{(by the previous case since } r > 0) \\ &= g^{\ell-r} \qquad \text{(by Lemma 9.5)} \\ &= g^{\ell+k} \qquad \text{(since } k = -r) \end{aligned}$$

□

Remark: One can prove by induction that if $a, b \in \mathbb{Z}$, then $(g^a)^b = g^{ab}$. The proof is left as an exercise.

The following result is essentially a Corollary of Theorem 9.6 but we state it as a Theorem because of its importance.

Theorem 9.7. *Let $(G, *)$ be a group and let $g \in G$. Then, the subset*

$$H := \{g^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Moreover, as a group $(H, *)$ is commutative.

Proof. We need to check the two conditions in the definition of a group. Suppose $h_1, h_2 \in H$ then there exist $k_1, k_2 \in \mathbb{Z}$ such that $h_1 = g^{k_1}$ and $h_2 = g^{k_2}$. But then, Theorem 9.6 says that

$$h_1 * h_2 = g^{k_1} * g^{k_2} = g^{k_1+k_2} \in H.$$

So, the first condition is satisfied.

Suppose now that $h \in H$. Then $h = g^k$ for some $k \in \mathbb{Z}$ and, again from Theorem 9.6 we have:

$$g^{-k} * g^k = g^{-k+k} = g^0 = e,$$

and similarly $g^k * g^{-k} = e$. Therefore

$$h^{-1} = g^{-k} \in H.$$

Finally, it is easy to see that, as a group, H is abelian. If $h_1, h_2 \in H$ we have that $h_1 = g^{k_1}$ and $h_2 = g^{k_2}$, for some $k_1, k_2 \in \mathbb{Z}$. But then, Theorem 9.6 says that

$$h_1 * h_2 = g^{k_1+k_2} = h_2 * h_1.$$

□

Remarks: The subgroup H in Theorem 9.7 is called the subgroup *generated* by g and g is called a *generator* of H. We will often denote by $\langle g \rangle$ the subgroup generated by g. If the operation of the group is addition then we will usually write $k \cdot g$ instead of g^k.

Example 9.8. If $G = \mathbb{Z}$ and $n \in \mathbb{Z}$ then the subgroup generated by n:

$$\langle n \rangle = \{k \cdot n : k \in \mathbb{Z}\}$$

coincides with the subgroup $n\mathbb{Z} \subseteq \mathbb{Z}$ defined in Example 9.3.

Example 9.9. Consider the multiplicative group $(\mathbb{Z}_5^*, \otimes)$ whose group table is given in Example 8.4. Note that every element g except $[1]$ has the property that $\langle g \rangle = \mathbb{Z}_5^*$. For example:

$$[2]^0 = [1]; \quad [2]^1 = [2]; \quad [2]^2 = [4]; \quad [2]^3 = [3].$$

Definition 9.10. A group G is said to be *cyclic* if there exists an element $g \in G$ such that

$$G = \langle g \rangle.$$

Example 9.11. The integers $(\mathbb{Z}, +)$ are a cyclic group since

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

In other words 1 is generator of $\mathbb{Z}$. Similarly, $n\mathbb{Z}$ is a cyclic subgroup with generator n (or $-n$).

By Example 9.9, the group $(\mathbb{Z}_5^*, \otimes)$ is cyclic. We may take any element different from 1 as a generator.

On the other hand, $(\mathbb{Q}^*, \cdot)$ is not a cyclic group. Suppose $r = p/q$ is a generator and assume, without loss of generality, that $\gcd(p, q) = 1$. Then if $x = r^n \in \langle r \rangle$, and $x = a/b$, $\gcd(a, b) = 1$ then either p/b of q/b. Therefore it is not possible to have $\mathbb{Q}^* = \langle r \rangle$ for any $r \in \mathbb{Q}^*$.

Theorem 9.12. *If G is a cyclic group then G is countable.*

Proof. Let G be a cyclic group and suppose g is a generator; i.e.

$$G = \langle g \rangle.$$

Let $f \colon \mathbb{Z} \to G$ be the map

$$f(n) = g^n.$$

Since g is a generator of G we know that f is a surjective map. If f is also injective then f is a bijection and G is denumerable.

Suppose then that f is not injective. Then there exist $m, n \in \mathbb{Z}$, $m \neq n$, such that $f(m) = f(n)$. We may assume without loss of generality that $m > n$. Then

$$g^m = g^n \Rightarrow g^m * g^{-n} = g^{m-n} = e.$$

Let now $A = \{k \in \mathbb{Z}_{>0} : g^k = e\}$. We have that $A \neq \emptyset$ (**Why?**). Let p be the smallest element in A. We now claim:

Claim: $f(m) = f(n)$ if and only if $m \equiv n \pmod{p}$

Let us prove the **Claim**. Suppose $m \equiv n \pmod{p}$, then $m = kp + n$ but then

$$f(m) = g^m = g^{kp+n} = (g^p)^k * g^n = e^k * g^n = g^n = f(n).$$

In particular, if r is the remainder of division of m by p, we have that $f(m) = f(r)$. Suppose then that $f(m) = f(n)$ and let $m \equiv r_1 \pmod{p}$, $m \equiv r_2 \pmod{p}$, with $0 \leq r_1, r_2 \leq p-1$. Then $f(r_1) = f(r_2)$ and if, say $r_1 < r_2$, it follows that $g^{r_2 - r_1} = e$ but since $r_2 - r_1 < p$ this is not possible. Therefore $r_1 = r_2$ and $m \equiv n \pmod{p}$.

Now, the claim means that the group G is bijectively equivalent to $\mathbb{Z}_p$ and, therefore, $|G| = p$. We will soon see that in fact G is more than bijectively equivalent to $\mathbb{Z}_p$. □

Remark: The arguments in the proof of Theorem 9.12 are very useful and merit a close and careful reading. For example, suppose G is any group, cyclic or not, and let $g \in G$ then we define the order of the element g to be ∞ if $g^m \neq e$ for any $m \in \mathbb{Z}_{>0}$ or to be the smallest element in

$$A := \{k \in \mathbb{Z}_{>0} : g^k = e\}$$

if A is not empty.

Corollary 9.13. *Let G be a group and suppose that $|G| = m$. Suppose $g \in G$ is an element of order m. Then $G = \langle g \rangle$; i.e. G is a cyclic group and g is a generator.*

Proof. Consider the elements $e, g, g^2, \ldots, g^{m-1}$. We claim that all these elements are different. Suppose $g^a = g^b$ with $0 \leq a < b \leq m-1$, then $g^{b-a} = e$ and $0 < b - a < m$ which is impossible since by definition of order m is the smallest positive integer k such that $g^k = 1$. □

Theorem 9.14 (**Fermat's Little Theorem**). *If p is prime and p does not divide a then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{9.1}$$

Proof. We will work in $\mathbb{Z}_p$, then the assumption that p does not divide a means that $[a] \neq [0]$ in $\mathbb{Z}_p$. We claim then that $[a]$ has order p in $(\mathbb{Z}_p, \oplus)$. Certainly $p \cdot [a] = [pa] = 0$, so we need to show that if $1 < r < p$ then $r \cdot [a] \neq [0]$. Suppose $r \cdot [a] = 0$ then p divides $r \cdot a$ but, since p is prime this means that either p divides a, which is not possible by assumption, or p divides r, which is impossible since $1 < r < p$. Therefore such r does not exist and p is the order of a. But if p is the order of $[a]$ it follows from Corollary 9.13 that $[a]$ generates $(\mathbb{Z}_p, \oplus)$. This means that the sets

$$\{[0], [a], [2a], [3a], \ldots, [(p-1]a]\}$$

and

$$\{[0], [1], [2], [3], \ldots, [p-1]\}$$

are equal. But then in $(\mathbb{Z}_p^*, \otimes)$:

$$[a] \otimes [2a] \otimes \cdots \otimes [(p-1)a] = [1] \otimes [2] \otimes \cdots \otimes [(p-1)]$$

which implies that

$$(1 \cdot 2 \cdot (p-1)) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot (p-1) \pmod{p}$$

and therefore

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Example 9.15. Let us compute the remainder of dividing 13^{46} by 23. Since 23 is prime and clearly does not divide 13, we have that

$$13^{22} \equiv 1 \pmod{23}.$$

Hence

$$13^{46} \equiv 13^2 = 169 \pmod{23}.$$

Since $169 = 7 \times 23 + 8$, we have that the remainder is 8.

Corollary 9.16. *If p is prime and p does not divide a then*

$$a^p \equiv a \pmod{p}.$$

Proof. Multiply both sides of identity (9.1) by a. □