今天上数列。等闲下来就去学生成函数来做数列题

最常见的问题：递推公式和通项公式的转换

1. 已知$\{a_n\}$通项为 $a_n=2^n+3^n$，验证其满足递推 $a_{n+2}=5a_{n+1}-6a_n \quad (n\geq 1)$

解：$2^{n+2}+3^{n+2}-5\times(2^{n+1}+3^{n+1})+6(2^n+3^n)$

$=(2-5)\times 2^{n+1}+(3-5)\times 3^{n+1}+3\times 2^{n+1}+2\times 3^{n+1}$

$=0$ $\quad\therefore$ 成立

2. 上n阶台阶，一次只能上一层 or 两层台阶，记上台阶方法种数为a_n，求$\{a_n\}$的递推公式。

解：思路：如何走到第n阶，分为两种可能

① 先走到$n-1$层，再走一级到n层 → 有a_{n-1}种

② 先走到$n-2$层，再走2级到n层 → 有a_{n-2}种

$\therefore a_n=a_{n-1}+a_{n-2}$

（也可以用组合数硬算）

等差数列：从第二项开始，数列的每一项与前一项的差均为一个固定的常数，这个常数称为公差，用d表示

递推公式：$a_{n+1}=a_n+d$

通项公式：$a_n=a_1+(n-1)d$

$$\begin{cases} a_n-a_{n-1}=d \\ a_{n-1}-a_{n-2}=d \\ \cdots \\ a_2-a_1=d \end{cases} \Rightarrow a_n-a_1=(n-1)d$$

累加法

等差数列前n项和：$S_n := \sum_{k=1}^{n} a_k = na_1+\frac{n(n-1)d}{2}$

$S_n=a_1+(a_1+d)+(a_1+2d)+\cdots+(a_1+(n-1)d)$

$=na_1+\frac{n(n-1)}{2}d$

若 $x_1+x_2=y_1+y_2=m$，则 $a_{x_1}+a_{x_2}=a_{y_1}+a_{y_2}$

$a_{x_1}+a_{x_2}=a_1+(x_1-1)d+a_1+(x_2-1)d$

$=2a_1+(m-2)d$

同理 $a_{y_1}+a_{y_2}=2a_1+(m-2)d$

$\Downarrow$

若 $x_1+x_2+\cdots+x_k=y_1+y_2+\cdots+y_k=m$

则 $a_{x_1}+a_{x_2}+\cdots+a_{x_k}=a_{y_1}+a_{y_2}+\cdots+a_{y_k}$

3. 已知某等差数列第二项为5，第5项11，求其通项公式

解：① $\begin{cases} a_2=a_1+d=5 \\ a_5=a_1+4d=11 \end{cases} \Rightarrow \begin{cases} d=2 \\ a_1=3 \end{cases}$

② $a_2+a_5=a_3+a_4=2a_{3.5}=2(a_3+\frac{1}{2}d)$

$=16$ $\quad\therefore a_3+\frac{1}{2}d=8 \quad \therefore 5+\frac{3}{2}d=8,\ d=2$

4. 一个有限项等差数列前三项和34，后三项和146，各项之和为390，求等差数列的项数。

解：$\begin{cases} a_1+a_2+a_3=3a+3d=34 \\ a_n+a_{n-1}+a_{n-2}=3a+(3n-6)d=146 \\ na_1+\frac{n(n-1)}{2}d=390 \end{cases}$

似乎方程很难解 所以我们换一种方法

$\begin{cases} a_1+a_2+a_3=34 \\ a_n+a_{n-1}+a_{n-2}=146 \end{cases} \Rightarrow a_n+a_1=\frac{180}{3}=60$

$\therefore S_n=a_1+\cdots+a_n=\frac{n}{2}(a_1+a_n)=390$

$\therefore n=13$

5. 对于等差数列$\{a_n\}$，记前n项和为S_n。若$S_{13}<0$，$S_{12}>0$，则数列中绝对值最小为第几项？

解：$S_{13}=13a_7<0 \quad \therefore a_7<0$

$S_{12}=6(a_1+a_{12})=6(a_6+a_7)>0$

$\therefore a_6>0 \quad \therefore d<0$

$\therefore |a_6|<|a_5|<\cdots<|a_1|$

$|a_7|<|a_8|<\cdots$

$\because a_6+a_7>0 \quad \therefore |a_6|>|a_7|$

$\therefore$ 最小为第7项。

等比数列：从第二项开始，数列的每一项与前一项的比均为一个固定的常数，这个常数称为公比，用q表示

递推公式：$a_{n+1}=qa_n$

通项公式：$a_n=a_1q^{n-1}$

$$\begin{cases} \frac{a_n}{a_{n-1}}=q \\ \frac{a_{n-1}}{a_{n-2}}=q \\ \cdots \\ \frac{a_2}{a_1}=q \end{cases} \Rightarrow \frac{a_n}{a_1}=q^{n-1}$$

累乘法

累加法和累乘法中d、q不一定相等，我们常用这两种方法求各种通项公式

例：$a_1=1$，$a_n=2a_{n-1}+1$，求通项

① 转化成累乘

$$\underbrace{a_n+1}_{b_n} = 2\underbrace{(a_{n-1}+1)}_{b_{n-1}} \quad \therefore b_n = 2b_{n-1}$$

$$\therefore b_n = 2^n b_1 = 2^n \quad \therefore a_n = 2^n - 1$$

② 转化成累加

$$\underbrace{\frac{a_n}{2^n}}_{b_n} = \underbrace{\frac{a_{n-1}}{2^{n-1}}}_{b_{n-1}} + \frac{1}{2^n} \quad \therefore b_n = b_{n-1} + \frac{1}{2^n}$$

$$\therefore b_n - b_1 = \frac{1}{2^n} + \frac{1}{2^{n-1}} + \cdots + \frac{1}{4}$$
$$= \frac{1}{4}\left(\frac{1}{2^{n-1}} - 1\right) / -\frac{1}{2}$$
$$= \frac{1}{2} - \frac{1}{2^n}$$

$$\therefore b_n = 1 - \frac{1}{2^n} \quad \therefore a_n = 2^n - 1$$

这里用了等比数列求和公式

等比数列求和公式

$$S_n = \sum_{k=1}^{n} a_k = \begin{cases} na_1, & q=1 \\ \frac{a_1(q^n-1)}{q-1}, & q \neq 1 \end{cases}$$

推导：$(q \neq 1)$

$$S_n = (1+q+q^2+\cdots+q^{n-1})a_1$$
$$qS_n = (q+q^2+\cdots+q^n)a_1$$
$$\therefore (q-1)S_n = (q^n-1)a_1$$
$$S_n = \frac{a_1(q^n-1)}{q-1}$$

例$_2$：$a_n = na_{n-1}+1$，$a_1=1$，求通项

解：$\underbrace{\frac{a_n}{n!}}_{b_n} = \underbrace{\frac{a_{n-1}}{(n-1)!}}_{b_{n-1}} + \frac{1}{n!}$

$$\therefore b_n = b_{n-1} + \frac{1}{n!}$$
$$\therefore b_n = 1 + \left(\frac{1}{n!} + \frac{1}{(n-1)!} + \cdots + \frac{1}{2}\right)$$
$$a_n = n! + (n-1)! + \cdots + 1$$

Maceradu，害我想了半天，上面这坨东西化简不了。具体见 OEIS：A007489（不过直猜有非初等形式

好，接下来我们推进 Napkin

§1.1 Definition and examples of groups

Prototypical example for this section: The additive group of integers $(\mathbb{Z},+)$ and the cyclic group $\mathbb{Z}/m\mathbb{Z}$. Just don't let yourself forget that most groups are non-commutative.

Definition 1.1.3. A **group** is a pair $G=(G,\star)$ consisting of a set of elements G, and a binary operation $\star$ on G, such that:

- G has an **identity element**, usually denoted 1_G or just 1, with the property that
$$1_G \star g = g \star 1_G = g \text{ for all } g \in G.$$
- The operation is **associative**, meaning $(a\star b)\star c = a\star(b\star c)$ for any $a,b,c\in G$. Consequently we generally don't write the parentheses.
- Each element $g\in G$ has an **inverse**, that is, an element $h \in G$ such that

注意，逆元是唯一的
$$g\star h = h\star g = 1_G.$$

Remark 1.1.4 (Unimportant pedantic point) — Some authors like to add a "closure" axiom, i.e. to say explicitly that $g\star h\in G$. This is implied already by the fact that $\star$ is a binary operation on G, but is worth keeping in mind for the examples below.

Remark 1.1.5 — It is not required that $\star$ is commutative ($a\star b=b\star a$). So we say that a group is **abelian** if the operation is commutative and **non-abelian** otherwise.

Example 1.1.6 (Non-Examples of groups)

- The pair $(\mathbb{Q}, \cdot)$ is NOT a group. (Here $\mathbb{Q}$ is rational numbers.) While there is an identity element, the element $0 \in \mathbb{Q}$ does not have an inverse.
- The pair $(\mathbb{Z}, \cdot)$ is also NOT a group. (Why?) Don't have an inverse.
- Let $\text{Mat}_{2\times 2}(\mathbb{R})$ be the set of 2×2 real matrices. Then $(\text{Mat}_{2\times 2}(\mathbb{R}), \cdot)$ (where $\cdot$ is matrix multiplication) is NOT a group. Indeed, even though we have an identity matrix

  $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

  we still run into the same issue as before: the zero matrix does not have a multiplicative inverse.

  (Even if we delete the zero matrix from the set, the resulting structure is still not a group: those of you that know some linear algebra might recall that any matrix with determinant zero cannot have an inverse.)

Example 1.1.7 (Complex unit circle)

Let S^1 denote the set of complex numbers z with absolute value one; that is

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

Then $(S^1, \times)$ is a group because

- The complex number $1 \in S^1$ serves as the identity, and
- Each complex number $z \in S^1$ has an inverse $\frac{1}{z}$ which is also in S^1, since $\left|z^{-1}\right| = |z|^{-1} = 1$.

There is one thing I ought to also check: that $z_1 \times z_2$ is actually still in S^1. But this follows from the fact that $|z_1 z_2| = |z_1| |z_2| = 1$.

Example 1.1.8 (Addition mod n)

Here is an example from number theory: Let $n > 1$ be an integer, and consider the residues (remainders) modulo n. These form a group under addition. We call this the **cyclic group of order** n, and denote it as $\mathbb{Z}/n\mathbb{Z}$, with elements $\overline{0}, \overline{1}, \dots$. The identity is $\overline{0}$.

同余等价类。我感觉这块难起来还得等讲到有限域的时候，那个因式分解有点哈人。不过估计等学到那也不觉得难了。

Example 1.1.9 (Multiplication mod p)

Let p be a prime. Consider the *nonzero residues modulo* p, which we denote by $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ is a group.

我怀疑上次看这问题可能我没看到这个 nonzero residues，现在看 quite easy.

> **Question 1.1.10.** Why do we need the fact that p is prime?

解：若不然，令其为 ab，$(\mathbb{Z}/ab\mathbb{Z})^\times=\{\bar{1},\bar{2},\cdots,\bar{a},\cdots\bar{b}\cdots,\overline{ab-1}\}$，$\bar{a}\bar{b}=0\notin(\mathbb{Z}/ab\mathbb{Z})^\times$，不满足乘的封闭性，$((\mathbb{Z}/ab\mathbb{Z})^\times,\times)$ 不是群。

Example 1.1.11 (General linear group)

Let n be a positive integer. Then $\mathrm{GL}_n(\mathbb{R})$ is defined as the set of $n\times n$ real matrices which have nonzero determinant. It turns out that with this condition, every matrix does indeed have an inverse, so $(\mathrm{GL}_n(\mathbb{R}),\times)$ is a group, called the **general linear group**.

(The fact that $\mathrm{GL}_n(\mathbb{R})$ is closed under $\times$ follows from the linear algebra fact that $\det(AB)=\det A\det B$, proved in later chapters.)

也就是不会出现行列式为0的情况

Example 1.1.12 (Special linear group)

Following the example above, let $\mathrm{SL}_n(\mathbb{R})$ denote the set of $n\times n$ matrices whose determinant is actually 1. Again, for linear algebra reasons it turns out that $(\mathrm{SL}_n(\mathbb{R}),\times)$ is also a group, called the **special linear group**.

Example 1.1.13 (Symmetric groups)

Let S_n be the set of permutations of $\{1,\dots,n\}$. By viewing these permutations as functions from $\{1,\dots,n\}$ to itself, we can consider *compositions* of permutations. Then the pair $(S_n,\circ)$ (here $\circ$ is function composition) is also a group, because

- There is an identity permutation, and
- Each permutation has an inverse.

The group S_n is called the **symmetric group** on n elements.

这玩意是我最烦的例子之一，特别是让我构造对称群与二面体群同构（尤其是不同构）的时候。

对于置换常用两套符号，一套是非常直观的：（以 $\{1,2,3\}$ 为例）

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

另一套稍微恶心一点，是 $(a_1a_2\cdots a_n)$ 的形式，满足以下规则：

$$\to a_1\to a_2\to a_3\to\cdots\to a_n$$

以上6种情况用这种方式写出来分别是：

$(1)\quad(2\,3)\quad(1\,2)\quad(1\,2\,3)\quad(1\,3)\quad(1\,3\,2)$

好处是计算合成相当方便。~~比如 $(1\,3\,4)\circ(3\,5\,7)\circ(6\,4\,7\,2\,5)$，则输入1后输出6~~

接下来我们来看 Dummit 上的例子。 这个例子犯了典型的错误，见下

Let $n = 13$ and let $\sigma \in S_{13}$ be defined by

$$\sigma(1) = 12,\quad \sigma(2) = 13,\quad \sigma(3) = 3,\quad \sigma(4) = 1,\quad \sigma(5) = 11,$$
$$\sigma(6) = 9,\quad \sigma(7) = 5,\quad \sigma(8) = 10,\quad \sigma(9) = 6,\quad \sigma(10) = 4,$$
$$\sigma(11) = 7,\quad \sigma(12) = 8,\quad \sigma(13) = 2.$$

我们有以下显然的方法：

Method	Example
To start a new cycle pick the smallest element of $\{1, 2, \ldots, n\}$ which has not yet appeared in a previous cycle — call it a (if you are just starting, $a = 1$); begin the new cycle: $(a$	$(1$
Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: $(a\,b$	$\sigma(1) = 12 = b$, $12 \neq 1$ so write: $(1\;12$
Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: $(a\,b\,c$ Repeat this step using the number c as the new value for b until the cycle closes.	$\sigma(12) = 8$, $8 \neq 1$ so continue the cycle as: $(1\;12\;8$

对题目中的例子进行操作，得 $\sigma = (1\;12\;8\;10\;4)(2\;13)(3)(5\;11\;7)(6\;9)$

（通常情况下，我们会去掉长度为1的置换，即 (n) 。因此 $\sigma = (1\;12\;8\;10\;4)(2\;13)(5\;11\;7)(6\;9)$）

For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order. For example, if $\sigma = (1\;12\;8\;10\;4)(2\;13)(5\;11\;7)(6\;9)$ is the element of S_{13} described before then

$$\sigma^{-1} = (4\;10\;8\;12\;1)(13\;2)(7\;11\;5)(9\;6).$$

Note：计算置换的合成，如 $\sigma\circ\tau$，要从右向左，先 τ 后 σ

例：计算 $(123)\circ(12)(34)$

解：$1 \to 2 \to 3$，$2 \to 1 \to 2$，$3 \to 4$，$4 \to 3 \to 1$ $\therefore$ $(123)\circ(12)(34) = (1\,3\,4)$

Dummit 对于每种群（初学者所能接触的）都进行了细致的介绍，简单且有良心（除了厚）。

这里再插一句，关于 $(\mathbb{Z}/n\mathbb{Z})^\times$，一般定义的是要求所有 $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ 与 n 互质，这样 n 没有必要为素数。

Example 1.1.14 (Dihedral group)

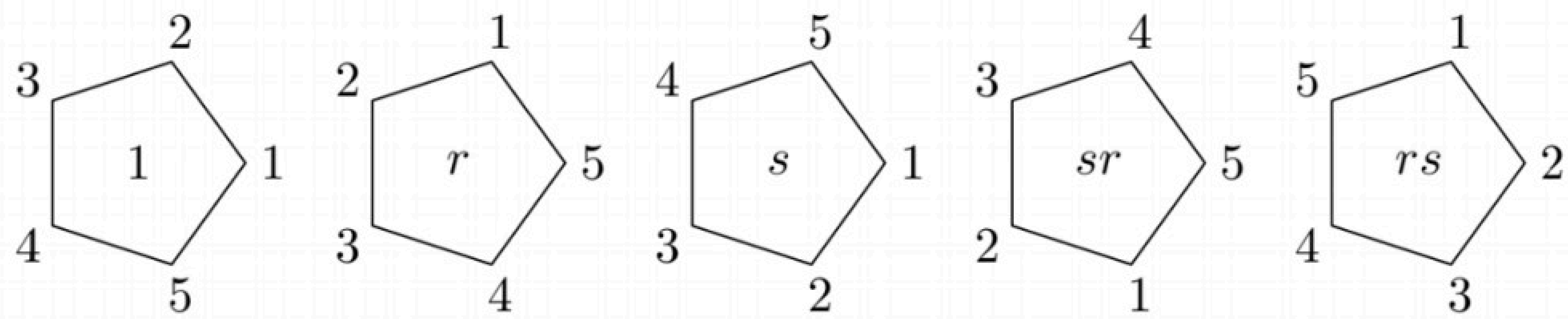
The **dihedral group of order** $2n$, denoted D_{2n}, is the group of symmetries of a regular n-gon $A_1A_2\ldots A_n$, which includes rotations and reflections. It consists of the $2n$ elements

$$\left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}.$$

The element r corresponds to rotating the n-gon by $\frac{2\pi}{n}$, while s corresponds to reflecting it across the line OA_1 (here O is the center of the polygon). So rs mean "reflect then rotate" (like with function composition, we read from right to left).

In particular, $r^n = s^2 = 1$. You can also see that $r^k s = sr^{-k}$.

Here is a picture of some elements of D_{10}.



Trivia: the dihedral group D_{12} is my favorite example of a non-abelian group, and is the first group I try for any exam question of the form "find an example…".

For each $n \in \mathbb{Z}^+$, $n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it. More precisely, we can describe the

贴切的说法

Then each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \dots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j. For instance, if s is a rotation of $2\pi/n$ radians clockwise about the center of the n-gon, then σ is the permutation sending i to $i+1$, $1 \leq i \leq n-1$, and $\sigma(n) = 1$. Now make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n-gon (note that we are viewing symmetries as functions on the n-gon, so st is just function composition — read as usual from right to left). If s, t effect the permutations σ, τ, respectively on the vertices, then st effects $\sigma \circ \tau$. The binary operation on D_{2n} is associative since composition of functions is associative. The identity of D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s (so if s effects permutation σ on the vertices, s^{-1} effects σ^{-1}). In the next paragraph we show

$$|D_{2n}| = 2n$$

and so D_{2n} is called the *dihedral group of order* $2n$. In some texts this group is written D_n; however, D_{2n} (where the subscript gives the order of the group rather than the number of vertices) is more common in the group theory literature.

(1) $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
(2) $|s| = 2$.
(3) $s \neq r^i$ for any i.
(4) $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

这里的$|a|$是元素的阶，$a^{|a|}=1$

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

i.e., each element can be written *uniquely* in the form $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n-1$.

典型的非阿贝尔群

(5) $rs = sr^{-1}$. [First work out what permutation s effects on $\{1, 2, \dots, n\}$ and then work out separately what each side in this equation does to vertices 1 and 2.] This shows in particular that r and s do not commute so that D_{2n} is non-abelian.
(6) $r^i s = sr^{-i}$, for all $0 \leq i \leq n$. [Proceed by induction on i and use the fact that $r^{i+1}s = r(r^i s)$ together with the preceding calculation.] This indicates how to commute s with powers of r.

所以这道题很显然了：

9. Prove that D_{24} and S_4 are not isomorphic.

解：首先注意到 $|D_{24}|=|S_4|=24$，两者之间肯定存在双射，但并不意味着同构；

同样可以构造一个映射 $\varphi: D_{24}\to S_4$，$r\to \underbrace{(1234)}_{\sigma}$，$s\to\underbrace{(12)}_{k}$，这里看起来~~没有~~很有问题，因为我们知道 D_{24} 由 $\langle r,s \mid r^{12}=s^2=1,\ sr=r^{-1}s\rangle$ 生成，S_4 由 $\langle \sigma,k \mid \sigma^4=k^2=1\rangle$ 生成，r^{12} 和 s^2 的结果被保留了，但 $sr=r^{-1}s$ 的关系没有被保留，即使对于 $r,s\in D_{24}$，$\sigma,k\in S_4$，$\varphi(a)\circ\varphi(b)=\varphi(a\cdot b)$，这个映射连同态都不是（其实怎么看都充满问题，刚刚那话当我没说）

一个表明二者不同构的理由是，$|r|=12$，而 S_4 中元素最高阶为 4。另外，比较同阶元素数量是否相等一般是可行的。

Example 1.1.15 (Products of groups)

Let $(G,\star)$ and $(H,*)$ be groups. We can define a **product group** $(G\times H,\cdot)$, as follows. The elements of the group will be ordered pairs $(g,h)\in G\times H$. Then

$$(g_1,h_1)\cdot(g_2,h_2)=(g_1\star g_2,h_1*h_2)\in G\times H$$

is the group operation.

Example 1.1.17 (Trivial group)

The **trivial group**, often denoted 0 or 1, is the group with only an identity element. I will use the notation $\{1\}$.

§1.2 Properties of groups

Prototypical example for this section: $(\mathbb{Z}/p\mathbb{Z})^\times$ *is possibly best.*

Proposition 1.2.4 (Inverse of products)

Let G be a group, and $a,b\in G$. Then $(ab)^{-1}=b^{-1}a^{-1}$.

Lemma 1.2.5 (Left multiplication is a bijection)

Let G be a group, and pick a $g\in G$. Then the map $G\to G$ given by $x\mapsto gx$ is a bijection. 被称为 cancellation law 消去律 $\Longleftrightarrow (ac=bc\Rightarrow a=b)$（因为是双射）

Example 1.2.7

Let $G=(\mathbb{Z}/7\mathbb{Z})^\times$ (as in Example 1.1.9) and pick $g=3$. The above lemma states that the map $x\mapsto 3\cdot x$ is a bijection, and we can see this explicitly:

$$\begin{aligned}
1 &\xmapsto{\times 3} 3 \pmod 7\\
2 &\xmapsto{\times 3} 6 \pmod 7\\
3 &\xmapsto{\times 3} 2 \pmod 7\\
4 &\xmapsto{\times 3} 5 \pmod 7\\
5 &\xmapsto{\times 3} 1 \pmod 7\\
6 &\xmapsto{\times 3} 4 \pmod 7.
\end{aligned}$$

§1.3 Isomorphisms

Prototypical example for this section: $\mathbb{Z} \cong 10\mathbb{Z}$.

Definition 1.3.1. Let $G = (G, \star)$ and $H = (H, *)$ be groups. A bijection $\phi : G \to H$ is called an **isomorphism** if

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

If there exists an isomorphism from G to H, then we say G and H are **isomorphic** and write $G \cong H$.

Example 1.3.3 (Primitive roots modulo 7)
As a nontrivial example, we claim that $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$. The bijection is

$$\phi(a \bmod 6) = 3^a \bmod 7.$$

- This map is a bijection by explicit calculation:

$$(3^0, 3^1, 3^2, 3^3, 3^4, 3^5) \equiv (1, 3, 2, 6, 4, 5) \pmod 7.$$

(Technically, I should more properly write $3^{0 \bmod 6} = 1$ and so on to be pedantic.)

- Finally, we need to verify that this map respects the group action. In other words, we want to see that $\phi(a+b) = \phi(a)\phi(b)$ since the operation of $\mathbb{Z}/6\mathbb{Z}$ is addition while the operation of $(\mathbb{Z}/7\mathbb{Z})^\times$ is multiplication. That's just saying that $3^{a+b \bmod 6} \equiv 3^{a \bmod 6} 3^{b \bmod 6} \pmod 7$, which is true.

a+b mod n = a mod n + b mod n

Example 1.3.4 (Primitive roots)
More generally, for any prime p, there exists an element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ called a **primitive root** modulo p such that $1, g, g^2, \dots, g^{p-2}$ are all different modulo p. One can show by copying the above proof that

$$\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{for all primes } p.$$

The example above was the special case $p = 7$ and $g = 3$.