Exponentiation

Let G be a group and let $g \in G$. For an integer $n > 0$ we denote:

- $g^n = \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ times}}$ (additive notation: $ng = \underbrace{g + g + \ldots + g}_{n \text{ times}}$)
- $g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{n \text{ times}}$ (additive notation: $(-n)g = \underbrace{-g - g - \ldots - g}_{n \text{ times}}$)
- $g^0 = e$ (additive notation: $0g = 0$)

Properties of exponentiation

- $g^{m+n} = g^m \cdot g^n$ (additive notation: $(m + n)g = (mg) + (ng)$)
- $g^{mn} = (g^m)^n$ (additive notation: $(mn)g = m(ng)$)

Definition 6.1

Let G be a group. An *order* of an element $g \in G$ is the smallest integer $n \geq 1$ such that $g^n = e$. We write: $|g| = n$.

If $g^n \neq e$ for all $n \geq 1$ then we say that g is an element of an *infinite order* and we write $|g| = \infty$.

Note. If $g^n = e$ then $g^{-1} = g^{n-1}$. In particular, if $g^2 = e$ then $g = g^{-1}$.

Exercise. Recall that the multiplication table of the dihedral group D_4 is as follows:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D'	D	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	I	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	I	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	I	R_{180}
D'	D'	V	D	H	R_{90}	R_{270}	R_{180}	I

Find the order of every element of D_4.

Exercise. Find the order of every element in the group $\mathbb{Z}_6$.

Theorem 6.2

If G is a finite group and $g \in G$ then $|g| < \infty$.

Proof. Consider the sequence

$$g^1, g^2, g^3, \cdots \subseteq G$$

Since G consists of finitely many elements, we must have $g^m = g^n$ for some $n > m$. This gives

$$\begin{aligned} g^{-m}g^m &= g^{-m}g^n \\ e &= g^{n-m} \end{aligned}$$

Thus $|g| \leq n - m < \infty$. $\square$

Theorem 6.3

If G is a group, $g \in G$ and $n \geq 1$ is an integer such that $g^n = e$, then $|g|$ divides n.

Proof. We have

$$n = |g| \cdot q + r$$

for some integers $q \geq 0$ and $0 \leq r < |g|$. We want to show that $r = 0$. Assume that it is not true. Then we have

$$e = g^n = g^{|g|\cdot q + r} = g^{|g|\cdot q} \cdot g^r = \left(g^{|g|}\right)^q \cdot g^r = e \cdot g^r = g^r$$

We obtain that $g^r = e$. This is however impossible, since $r < |g|$. $\square$

Theorem 6.4

If G is a group, and $a, b \in G$ are elements such that $|a|, |b| < \infty$ and $ab = ba$ then $|ab|$ divides $|a| \cdot |b|$.

Proof. Let $|a| = m$ and $|b| = n$. We have

$$(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n \cdot (b^n)^m = e^n \cdot e^m = e$$

By Theorem 6.3 we get that $|ab|$ divides $mn = |a| \cdot |b|$. $\square$

Example. In the dihedral group D_4 take $a = R_{90}$, $b = R_{180}$. Then $a \cdot b = R_{90} \cdot R_{180} = R_{270}$ We have $|R_{90}| = 4$, $|R_{180}| = 2$, so $|R_{90}| \cdot |R_{180}| = 8$ which is divisible by $|R_{270}| = 4$.

Example. Theorem 6.4 is not true in general if $ab \neq ba$. Take for example a, b to be two different reflections in the dihedral group D_3. Then $|a| = |b| = 2$, so $|a| \cdot |b| = 4$, but $|ab| = 3$.

As another example, in the group $GL(2, \mathbb{R})$ take matrices

$$A = \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Then $|A| = 2$ and $|B| = 2$ but $|AB| = \infty$.

Theorem 6.5

If G is a group, and $a \in G$ is element such that $|a| = n < \infty$ then

$$|a^k| = \frac{n}{\gcd(n,k)}$$

Exercise. Compute the order of the element $6 \in \mathbb{Z}_{10}$.

Proof of Theorem 6.5. Let $|a^k| = r$. Then r is the smallest positive integer such that $\left(a^k\right)^r = a^{kr} = e$. Using Theorem 6.3 we obtain that r is the smallest positive integer such that $n|kr$. This means that kr is the least common multiple of n and k: $kr = \operatorname{lcm}(n,k)$. This gives:

$$kr = \operatorname{lcm}(n,k) = \frac{nk}{\gcd(n,k)}$$

and so $r = \dfrac{n}{\gcd(n,k)}$. $\square$