Notation

Additive Groups:

$$\begin{aligned} 0 &= \text{identity} \\ -a &= \text{inverse of } a \\ 0a &= 0 \\ na &= a + a + \ldots + a \quad \text{(n times)} \\ -na &= (-a) + (-a) + \ldots + (-a) = n(-a) \end{aligned}$$

Multiplicative Groups:

$$\begin{aligned} 1 &= \text{identity} \\ a^{-1} &= \text{inverse of } a \\ a^0 &= 1 \\ a^n &= aa \ldots a \quad \text{(n times)} \\ a^{-n} &= (a^{-1})(a^{-1}) \ldots (a^{-1}) = (a^{-1})^n \end{aligned}$$

Unless the form of the group is explicitly stated, the multiplicative (juxtaposition) notation is generally used by default. An exception is for abelian groups, where the additive notation is preferred.

Theorem

Let G be a group and $n \in \mathbb{Z}$:

$$\forall\, a \in G, a^{-n} = (a^n)^{-1}$$

Proof

Assume $a \in G$

Case 1: $n = 0$

$$a^{-0} = a^0 = e = e^{-1} = (a^0)^{-1}$$

Case 2: $n > 0$

Proof by induction on n:

Base: $n = 1$:

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

Assume $a^{-n} = (a^n)^{-1}$

Consider $a^{-(n+1)}$:

$$a^{-(n+1)} = (a^{-1})^{n+1} = (a^{-1})^n a^{-1} = a^{-n}a^{-1} = (a^n)^{-1}a^{-1} = (aa^n)^{-1} = (a^{n+1})^{-1}$$

Case 3: $n < 0$

Let $m = -n$
$m > 0$
$a^{-n} = a^m = [(a^m)^{-1}]^{-1} = (a^{-m})^{-1} = (a^{-(-n)})^{-1} = (a^n)^{-1}$

Corollary

Let G be a group and $n \in \mathbb{Z}$:

$$\forall\, a \in G, a^n a^{-n} = e$$

Proof

Assume $a \in G$
$a^n a^{-n} = a^n (a^n)^{-1} = e$

Theorem

Let G be a group and $n, m \in \mathbb{Z}$:

$$\forall\, a \in G, a^m a^n = a^{m+n}$$

Proof

Assume $a \in G$

Case 1: $m = 0$

$$a^0 a^n = ea^n = a^n = a^{0+n}$$

Case 2: $n = 0$

$$a^m a^0 = a^m e = a^m = a^{m+0}$$

Case 3: $m, n > 0$

Proof by induction on n for a fixed value of m:

Base: $n = 1$:

$$a^m a^1 = a^m a = a^{m+1}$$

Assume $a^m a^n = a^{m+n}$

Consider $a^m a^{n+1}$:

$$a^m a^{n+1} = a^m (a^n a) = (a^m a^n)a = a^{m+n}a = a^{(m+n)+1} = a^{m+(n+1)}$$

Case 4: $m, n < 0$

Let $h = -m$ and $k = -n$
$h, k > 0$
$a^m a^n = a^{-h} a^{-k} = (a^h)^{-1}(a^k)^{-1} = (a^k a^h)^{-1} = (a^{k+h})^{-1} = (a^{h+k})^{-1} = a^{-(h+k)}$
$a^m a^n = a^{-(-m-n)} = a^{m+n}$

Case 5: $m > 0$ and $n < 0$

Case 1: $m = |n|$

$m + n = 0$
$n = -m$
$a^m a^n = a^m a^{-m} = e = a^0 = a^{m-m} = a^{m-(-n)} = a^{m+n}$

Case 2: $m > |n|$

$(a^m a^n)(a^{m+n})^{-1} = [a^m a^{-(-n)}](a^{m+n})^{-1} = a^m[(a^{-n})^{-1}(a^{m+n})^{-1}] = a^m(a^{m+n}a^{-n})^{-1}$
But $m + n > 0$ and $-m > 0$, so
$(a^m a^n)(a^{m+n})^{-1} = a^m[a^{(m+n)-n}]^{-1} = a^m(a^m)^{-1} = e$
By uniqueness of the inverse, $a^m a^n = [(a^{m+n})^{-1}]^{-1}$
$\therefore a^m a^n = a^{m+n}$

Case 3: $m < |n|$

$(a^{m+n})^{-1}(a^m a^n) = (a^{m+n})^{-1}[a^{-(-m)}a^n] = [(a^{m+n})^{-1}(a^{-m})^{-1}]a^n = (a^{-m}a^{m+n})^{-1}a^n$
But $-m < 0$ and $m + n < 0$, so
$(a^{m+n})^{-1}(a^m a^n) = [a^{-m+(m+n)}]^{-1}a^n = (a^n)^{-1}a^n = e$
By uniqueness of the inverse, $a^m a^n = [(a^{m+n})^{-1}]^{-1}$
$\therefore a^m a^n = a^{m+n}$

Case 6: $m < 0$ and $n > 0$

Case 1: $|m| = n$

$m + n = 0$
$n = -m$
$a^m a^n = a^m a^{-m} = e = a^0 = a^{m-m} = a^{m-(-n)} = a^{m+n}$

Case 2: $|m| < n$

$(a^{m+n})^{-1}(a^m a^n) = (a^{m+n})^{-1}[a^{-(-m)}a^n] = [(a^{m+n})^{-1}(a^{-m})^{-1}]a^n = (a^{-m}a^{m+n})^{-1}a^n$
But $-m > 0$ and $m + n > 0$, so
$(a^{m+n})^{-1}(a^m a^n) = [a^{-m+(m+n)}]^{-1}a^n = (a^n)^{-1}a^n = e$
By uniqueness of the inverse, $a^m a^n = [(a^{m+n})^{-1}]^{-1}$
$\therefore a^m a^n = a^{m+n}$

Case 3: $|m| > n$

$(a^m a^n)(a^{m+n})^{-1} = [a^m a^{-(-n)}](a^{m+n})^{-1} = a^m[(a^{-n})^{-1}(a^{m+n})^{-1}] = a^m(a^{m+n}a^{-n})^{-1}$
But $m + n < 0$ and $-n < 0$, so
$(a^m a^n)(a^{m+n})^{-1} = a^m[a^{(m+n)-n}]^{-1} = a^m(a^m)^{-1} = e$

By uniqueness of the inverse, $a^m a^n = [(a^{m+n})^{-1}]^{-1}$
$\therefore a^m a^n = a^{m+n}$

Corollary

Let G be a group and $n, m \in \mathbb{Z}$:

$\forall\, a \in G, a^m a^n = a^n a^m$

Proof

Assume $a \in G$
$a^m a^n = a^{m+n} + a^{n+m} = a^n a^m$

Theorem

Let G be a group and $n, m \in \mathbb{Z}$:

$\forall\, a \in G, (a^m)^n = a^{mn}$

Proof

Assume $a \in G$

Case 1: $n = 0$

$(a^m)^0 = e = a^0 = a^{m0}$

Case 2: $n > 0$

Proof by induction on n:

Base: $n = 1$

$(a^m)^1 = a^m = a^{m1}$

Assume $(a^m)^n = a^{mn}$

Consider $(a^m)^{n+1}$

$(a^m)^{n+1} = (a^m)^n (a^m) = a^{mn} a^m = a^{mn+m} = a^{m(n+1)}$

Case 3: $n < 0$

Let $k = -n$
$k > 0$
$(a^m)^n = (a^m)^{-k} = [(a^m)^k]^{-1} = (a^{mk})^{-1} = a^{-mk} = a^{-m(-n)} = a^{mn}$

Thus, all of the exponent rules work as expected.

Example

$a^{-2}a^5 = (a^{-1})(a^{-1})aaaaa = (a^{-1})eaaaa = (a^{-1})aaaa = eaaa = aaa = a^3$

Theorem

Let G be an abelian group and $n \in \mathbb{Z}$:

$$\forall\, a, b \in G, (ab)^n = a^n b^n$$

Proof

Assume $a, b \in G$.

Case 1: $n = 0$

$$(ab)^0 = e = ee = a^0 b^0$$

Case 2: $n > 0$

Proof by induction on n:

Base: $n = 1$

$$(ab)^1 = ab = a^1 b^1$$

Assume $(ab)^n = a^n b^n$

Consider $(ab)^{n+1}$

$$\begin{aligned} (ab)^{n+1} &= (ab)(ab)^n \\ &= (ab)(a^n b^n) \\ &= (ab)(b^n a^n) \\ &= a(bb^n)a^n \\ &= ab^{n+1}a^n \\ &= aa^n b^{n+1} \\ &= a^{n+1}b^{n+1} \end{aligned}$$

Case 3: $n < 0$

Let $m = -n$
$(ab)^n = (ab)^{-m} = [(ab)^m]^{-1}$
But $m > 0$, so:
$(ab)^n = (a^m b^m)^{-1} = (b^m)^{-1}(a^m)^{-1} = b^{-m}a^{-m} = b^{-(-n)}a^{-(-n)} = b^n a^n = a^n b^n$

Theorem

Let G be a finite group with order m:

$$\forall\, a \in G, \exists\, n \in \mathbb{Z}^+, a^n = e$$

Proof

Assume $a \in G$

Consider the set $S = \{a^0 = e, a, a^2, a^3, \ldots, a^m\}$
By closure, $S \subseteq G$
$|S| = m + 1$, so at least one of the elements in S is repeated
If the repeated element is e then done
Otherwise, assume $a^i = a^j$, where $i < j$
$a^i a^{-i} = a^j a^- i$
$a^0 = a^{j-i}$
$e = a^{j-i}$
Let $n = j - i$
$0 < n < m$ so $a^n \in S$
$\therefore \exists n \in \mathbb{Z}^+, a^n = e$