Cyclic Groups: Prop: Every cyclic gp is abelian.

Proof: Let $G=\langle a\rangle$ be a cyclic gp and let $x,y\in G$. Say $x=a^n$, $y=a^m$ for $n,m\in\mathbb{Z}$. Then $xy=a^na^m=a^{n+m}=a^{m+n}=yx$. □

Thm: Every subgp of a cyclic gp is cyclic.

proof: Let $G=\langle a\rangle=\{a^n : n\in\mathbb{Z}\}$ be a cyclic gp.

Note that now following Boltje's notes!

Let $H\subseteq G$ be a subgp.

If $H=\{1\}$, then $H=\langle 1\rangle$ is cyclic and we are done.

Assume $H\neq\{1\}$.

Let n be the least positive integer such that

$$a^n\in H \quad \text{and} \quad a^n\neq 1$$

Such an n exists because $H\neq\{1\}$, $G=\{a^n : n\in\mathbb{Z}\}$, and H is closed under inversion.

We claim that $H=\langle a^n\rangle$. Since $a^n\in H$, $\langle a^n\rangle\subseteq H$.

Now let $h\in H$. Since $G=\{a^n : n\in\mathbb{Z}\}$, $h=a^m$ for some $m\in\mathbb{Z}$.

Divide m by n with remainder to get

$$m=qn+r,\quad q,r\in\mathbb{Z},\quad 0\le r\le n-1$$

Then $$a^m=a^{qn+r}=a^{qn}a^r$$

$$a^n\in H \Rightarrow (a^n)^q=a^{qn}\in H \Rightarrow a^{-qn}\in H$$

so $$a^{-qn}a^m=a^r\in H.$$ By minimality of n and that $0\le r\le n-1$, we must have that $a^r=1$. Hence $a^m=a^{qn}$, so $a^m\in\langle a^n\rangle$. □

Cor: The subgps of $(\mathbb{Z},+)$ are the groups $\langle n\rangle = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ with $n \in \mathbb{N}_0$. Moreover, if $n,m \in \mathbb{N}_0$ with $m\mathbb{Z} = n\mathbb{Z}$, then $m=n$.

proof: Let H be a subgp of $\mathbb{Z}$. By previous Thm, $H = \langle n\rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Now $n\mathbb{Z} = (-n)\mathbb{Z}$, so we may take $n \in \mathbb{N}_0$. Conversely, if $n \in \mathbb{N}_0$, then $H = \langle n\rangle$ is a subgp of $\mathbb{Z}$.

Let $n,m \in \mathbb{N}_0$ be s.t. $n \neq m$. WLOG say $n < m$. Then $n\mathbb{Z} \neq m\mathbb{Z}$ because n is not a multiple of m, so $n \notin m\mathbb{Z}$.

Thm: Let $a,b \in \mathbb{N}$. Then in $(\mathbb{Z},+)$, we have

$$\langle a,b\rangle = \langle \gcd(a,b)\rangle$$

and there exist $m,n \in \mathbb{Z}$ such that

$$\gcd(a,b) = ma + nb$$

Intuition:
$\langle a\rangle = a\mathbb{Z}$ = multiples of a
$\langle b\rangle = b\mathbb{Z}$ = multiples of b
$\langle a,b\rangle \supseteq$ multiples of a and b?

proof: Note that $\langle a,b\rangle = \{ma + nb : m,n \in \mathbb{Z}\}$.
By previous cor, $\exists!\, d \in \mathbb{N}_0$ s.t. $\langle d\rangle = \langle a,b\rangle$. Since $a,b \in \mathbb{N}$, $\langle a,b\rangle \neq \langle 0\rangle$, so $d \in \mathbb{N}$. We have then that $d = ma + nb$ for some $m,n \in \mathbb{Z}$, we just need to show that $d = \gcd(a,b)$.

First d divides a,b: $a \in \langle a,b\rangle = \langle d\rangle$, so $\exists k \in \mathbb{Z}$ s.t. $a = kd$.
$b \in \langle a,b\rangle = \langle d\rangle$, so $\exists l \in \mathbb{Z}$ s.t. $b = ld$.

Second, let $e \in \mathbb{Z}$ be s.t. $e \mid a$ and $e \mid b$. We need to show that $e \mid d$.

$e \mid a$ means $\exists\, k \in \mathbb{Z}$ s.t. $a = ke$
$e \mid b$ means $\exists\, l \in \mathbb{Z}$ s.t. $b = le$

Then $\quad d = ma + nb = mke + nle = (mk+nl)e$, so e divides d. $\square$

Lemma: Let G be a group, let a be an element of G, and let $n \in \mathbb{N}$ be s.t. $a^n = 1$. Then $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$. In particular, $\langle a \rangle$ has at most n elements.

Proof: By definition of $\langle a \rangle$, as $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, we have

$$\{1, a, a^2, \dots, a^{n-1}\} \subseteq \langle a \rangle$$

Conversely, let $b \in \langle a \rangle$, so $b = a^m$ for some $m \in \mathbb{Z}$.

Divide m by n with remainder to get

$$m = qn + r, \quad q, r \in \mathbb{Z}, \quad 0 \le r \le n-1$$

Then

$$a^m = a^{qn+r} = a^{nq} a^r = (a^n)^q a^r = 1^q a^r = a^r \in \{1, a, a^2, \dots, a^{n-1}\} \square$$

Thm: Let $G = \langle a \rangle$ be an infinite cyclic gp.

(a) If $k \ne l$, then $a^k \ne a^l$.

(b) The function

$$f : \mathbb{Z} \to G. \qquad k \mapsto a^k.$$

is an isomorphism between $(\mathbb{Z}, +)$ and G. Thus every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Proof: (a) Proof by contradiction: Let $k, l \in \mathbb{Z}$ be s.t. $k \ne l$ and $a^k = a^l$. WLOG assume $k > l$.

Then $\quad a^{k-l} = 1$ by multiplying both sides by a^{-l}.

Now $k-l \in \mathbb{N}$ since $k > l$, so by previous lemma $|G| \leq n$ contradicting that G is infinite.

(b) First f is a hom:

$$f(k+l) = a^{k+l}$$
$$= a^k a^l$$
$$= f(k) f(l)$$

f is surjective by def. of $\langle a \rangle$.

By (a), if $f(k) = f(l)$ then

$$a^k = a^l \quad \text{then}$$
$$k = l.$$

So f is injective. Hence f is an isom. $\square$

Def: Let G be a gp and let $a \in G$. The order of a is defined as the smallest $n \in \mathbb{N}$ s.t. $a^n = 1$. If no such n exists, we define the order of a to be ∞. We denote the order of a by $o(a)$. The order of the gp. $*$

$*$ Bad terminology: For a finite gp, the size of the gp is also called the order of the gp.

Example: (i) Let a be an element in a gp. Then $o(a) = 1$ iff $a = 1$.

(ii) The element $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ in $Sym(3)$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id$$

Therefore $o(\sigma) = 3$.

(iii) $3+n\mathbb{Z} \in \mathbb{Z}/12\mathbb{Z}$ use $\bar{3} \in \mathbb{Z}/12\mathbb{Z}$

Notice the additive notation instead of multiplicative.

$2\cdot\bar{3} = \bar{3}+\bar{3} = \bar{6}$

$3\cdot\bar{3} = \bar{3}+\bar{6} = \bar{9}$

$4\cdot\bar{3} = \bar{3}+\bar{9} = \overline{12} = 0$

$o(\bar{3}) = 4$

<u>Thm</u>: Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(a) One has $G = \{1, a, \ldots, a^{n-1}\}$, the elements $1, a, a^2, \ldots, a^{n-1}$ are pairwise distinct, and $o(a) = n = |G|$.

(b) For all integers k and l, one has: $a^k = a^l$ iff $k \equiv l \mod n$.

(c) The function

$$f: \mathbb{Z}/n\mathbb{Z} \longrightarrow G$$
$$\bar{k} \longmapsto a^k$$

is an isomorphism between $(\mathbb{Z}/n\mathbb{Z}, +)$ and G. Therefore every cyclic gp of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

<u>proof</u>: (a) Since G has order n, the $n+1$ elements $1, a, a^2, \ldots, a^n$ cannot be pairwise distinct. Therefore there exists k, l with $0 \le k < l \le n$ s.t. $a^k = a^l$. Then multiplying both sides by a^{-k} gives

$$a^{l-k} = 1$$

By previous lemma, G has at most $l-k$ elements. But $l-k \le n$, so ~~there is~~ so $l-k = n$ implying $l = n$ and $k = 0$. Hence $a^n = 1$ and by previous lemma $G \subseteq \{1, a, \ldots, a^{n-1}\}$. Since both sets have size n, we get that $G = \{1, a, \ldots, a^{n-1}\}$.

Since $a^n = 1$ and $a^i \neq 1$ for $1 \le i \le n-1$, we get that $o(a) = n$.

(b) $a^k = a^l$ iff $a^{k-l} = 1$

divide $k-l$ by n with remainder gives

$k-l = qn + r$ where $q, r \in \mathbb{Z}$, $0 \le r \le n-1$

Then $a^{k-l} = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = 1^q a^r = a^r$
we have that $1, a, a^2, \ldots, a^{n-1}$ are all distinct, so $0 \le r \le n-1$ and
$a^r = 1$ implies $r = 0$.
Hence we shown that

$a^{k-l} = 1$ implies $k \equiv l \mod n$ since n divides $k-l$.
Conversely if $k \equiv l \mod n$, then $k-l = nq$ for some q, so

$a^{k-l} = a^{nq} = (a^n)^q = 1^q = 1$

so $a^{k-l} = 1$.

(c) By part (b) the function is well-defined:
If $\bar{k} = \bar{l}$, then $k \equiv l \mod n$, so $f(\bar{k}) = a^k = a^l = f(\bar{l})$.
f is surjective since $G = \langle a \rangle$. Therefore since $|\mathbb{Z}/n\mathbb{Z}| = |G| = n$,
f is a bijection. It remains to show f is a homomorphism.
This is easy

$f(\bar{k} + \bar{l}) = f(\overline{k+l}) = a^{k+l} = a^k a^l = f(\bar{k}) f(\bar{l})$. $\square$

Cor: Let G be a gp and let a be an element of G. Then $o(a) = |\langle a \rangle|$.

proof: If $\langle a \rangle$ is a gp of infinite order, then by the Thm on ~~cyclic~~ cyclic groups of infinite order, $a^k \neq a^l$ if $k \neq l$. In particular

$$a^k \neq 1 \quad \text{for all } k > 0$$

Hence $o(a) = \infty = |\langle a \rangle|$.

If $\langle a \rangle$ is a gp of finite order n, then by previous Thm, $n = |\langle a \rangle| = o(a)$. $\square$

Cor: Let G be a gp and let $a \in G$ be an element of order n. Then

$$a^k = 1 \quad \text{iff} \quad n \text{ divides } k.$$

proof: Divide n into k with remainder, to get $k = nq + r$, $q, r \in \mathbb{Z}$, $0 \leq r \leq n-1$. Then

$$a^k = a^{nq+r} = a^{nq} a^r = a^r$$

$a^r = 1$ iff $r = 0$ since $\langle a \rangle = \{1, a, \dots, a^{n-1}\}$ and the $1, a, \dots, a^{n-1}$ are all distinct. Therefore $a^k = a^r = 1$ iff n divides k.

Prop: Let G be a group and $a \in G$ an element of finite order n. Let $k \in \mathbb{N}$. Then $o(a^k) = n / \gcd(k, n)$.

proof: Let $d = \gcd(k, n)$. We need to determine the smallest $m \in \mathbb{N}$ s.t.

$$(a^k)^m = 1$$

By previous Cor,

$$(a^k)^m = a^{km} = 1 \text{ iff } n \text{ divides } km$$

Since d divides n and k,

$$n \text{ divides } km \text{ iff } \frac{n}{d} \text{ divides } \frac{k}{d}m$$

Since $d = \gcd(k,n)$, $\frac{n}{d}$ and $\frac{k}{d}$ have no common factors.

Therefore

$$\frac{n}{d} \text{ divides } \frac{k}{d}m \text{ iff } \frac{n}{d} \text{ divides } m$$

We've shown $(a^k)^m = 1$ iff $\frac{n}{d}$ divides m.

The smallest $m \in \mathbb{N}$ s.t. $\frac{n}{d}$ divides m is $m = \frac{n}{d}$. $\square$

<u>Cor</u>: Let $G = \langle a \rangle$ be a finite gp of order n. One has $G = \langle a^k \rangle$ iff $\gcd(k,n) = 1$.

<u>Proof</u>: By previous prop, $o(a^k) = \frac{n}{\gcd(k,n)}$, $\frac{n}{\gcd(k,n)} = n$ iff $\gcd(k,n) = 1$. $\square$

Translate previous two statements to $\mathbb{Z}/n\mathbb{Z}$:

<u>Prop</u>: $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$, so $o(\bar{k}) = n/\gcd(k,n)$. $o(\bar{k}) = |\langle \bar{k} \rangle|$.

<u>Cor</u>: $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{k}$ iff $\gcd(k,n) = 1$.

Example

(i) what are the generators of the gp $(\mathbb{Z}/12\mathbb{Z}, +)$?

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}$

generators are $\overline{1}, \overline{5}, \overline{7}, \overline{11}$

(ii) what are the subgps of $(\mathbb{Z}/12\mathbb{Z}, +)$?

All subgps are cyclic, so need to write down the cyclic subgp generated by each element and identify the ones that are the same.

$$\boxed{\begin{array}{l} \mathbb{Z}/12\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle \\ \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = \langle \overline{10} \rangle \\ \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = \langle \overline{9} \rangle \\ \langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\} = \langle \overline{8} \rangle \\ \langle \overline{6} \rangle = \{\overline{0}, \overline{6}\} \end{array}}$$

These are all the subgps.

$\langle \overline{8} \rangle = \{\overline{0}, \overline{8}, \overline{16} = \overline{4}\} = \langle \overline{4} \rangle$

$\langle \overline{9} \rangle = \{0, \overline{9}, \overline{18} = \overline{6}, \overline{15} = \overline{3}\} = \langle \overline{3} \rangle$

$\langle \overline{10} \rangle = \{0, \overline{10}, \overline{20} = \overline{8}, \overline{18} = \overline{6}, \overline{16} = \overline{4}, \overline{14} = \overline{2}\} = \langle \overline{2} \rangle$