Chris Hayduk 9/17

Lecture 7, Exercise B

1a. We have $H = \langle x^a \rangle$

$$= \{(x^a)^n \mid n \in \mathbb{Z}\}$$

Since $x \in H$, we have

$$x = (x^a)^n = x^{an}$$

for some $n \in \mathbb{Z}$

b. We have

$$1 = x^{an-1}$$

c. Since $|x|$ infinite, we have

$$an - 1 = 0$$

$$\Rightarrow an = 1$$

Note that $an = 1$ iff

$$a = -1, \quad n = -1$$

$$a = 1, \quad n = 1$$

Hence $a = \pm 1$

2. Suppose $x^m = 1$ and $x^n = 1$

Let $k = (m, n)$

Then $k \mid m$ and $k \mid n$, and $\forall \ell$ s.t. $\ell \mid m$ and $\ell \mid n$, $\ell \mid k$.

Now assume $|x| = j$

Then, since $x^m = 1$ and $x^n = 1$, we have

$$j \mid m \quad \text{and} \quad j \mid n$$

and, from the above, we have,

$$j \mid k$$

Hence,

$$x^k = x^{(m,n)} = 1$$

3. Proof of (I)

a. We have $K \leq H$ where

$$H = \{x^{\ell} \mid \ell \in \mathbb{Z}\}$$

Thus $\forall y \in K$, we have

$$y = x^{m}$$

for some $m \in \mathbb{Z}$

Since $K \neq 1$, $\exists x^{a} \in K$ s.t.

$$x^{a} \neq 1$$

So $a > 0$ and $a \in \mathbb{Z}$

b. Well-ordering Principle: If A is any nonempty subset of $\mathbb{Z}^{+}$, there is some element $m \in A$ s.t. $m \leq a$ $\forall a \in A$ (m is called the minimal element of A)

We have that $P = \{b \in \mathbb{Z}_{>0} \mid x^{b} \in K\}$

Every $b \in \mathbb{Z}^{+}$, so just need to show that P is non-empty to apply well-ordering.

From part a), have that
$\exists x^a \in K$ s.t. $a > 0$.

Hence, $a \in P$ and $P \neq \emptyset$.

So P must have a least element.

c. Let d be minimal element of P $(x^d \in K)$ and write:

$$a = qd + r \quad q, r \in \mathbb{Z} \text{ and } 0 \le r < d$$

We then have

$$r = a - qd$$

So $$x^r = x^{a-qd}$$

$$= x^a x^{-qd}$$

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

We know $x^a \in K$. Since $x^d \in K$ and K a group, $(x^{qd})^{-1} \in K$.

So $x^r \in K$

But $r < d$, the minimal element of P. So r cannot be in P and therefore must be 0.

d. x^a was an arbitrary element of K.

Hence, every element $x^a \in K$ can be written as

$$a = qd$$

for some $q \in \mathbb{Z}$

Thus, K is generated by x^d and

$$K = \langle x^d \rangle$$

Proof of (III)

a. Let $d = n/a$

We have $(x^d)^a = (x^{n/a})^a$

$$= x^n = 1$$

Now let $b < a$. Then

$$bd < ad = n$$

So $x^{bd} \neq 1$ since $|H| = n$

So $|\langle x^d \rangle| = a$

b. By (I), $\exists$ a generator x^b of K s.t. $b=0$ if $K=1$ or b is the least positive integer s.t. $x^b \in K$

c. Proposition 5: Let G be a group, let $x \in G$, let $a \in \mathbb{Z} - \{0\}$

1) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$

2) In particular, if $|x| = n < \infty$ and a is a positive integer s.t. $a | n$, then $|x^a| = \frac{n}{a}$

So by Prop 5:

$$|x^b| = \frac{n}{(n,b)}$$

Since $|K| = a$:

$$a = \frac{n}{(n,b)}$$

$$\Rightarrow \frac{n}{a} = (n,b)$$

$$\Rightarrow d = (n,b)$$

So $|x^b| = \frac{n}{d}$

2. We have $d = \gcd(n, b)$

Hence $d \mid b$.

Since $d \mid b$, $\exists\, m \in \mathbb{Z}_{>0}$ s.t

$$b = md$$

So $x^b = x^{md}$

Hence any power of x^b can be written as

$$x^{ib} = x^{imd} = x^{(im)d}$$

$\forall i \in \mathbb{Z}$

Thus, for every element $x^{ib} \in K$ we have $x^{ib} = x^{(im)d} \in \langle x^d \rangle$

Hence, $K = \langle x^b \rangle$ is contained in $\langle x^d \rangle$

e. We have $|\langle x^d \rangle| = a$. Assume $|K| = a$

We also have $x^b \in \langle x^d \rangle \Rightarrow K = \langle x^b \rangle \leq \langle x^d \rangle$

Since $|\langle x^d \rangle| = a$,

$$K = \langle x^d \rangle$$

Hence $\langle x^d \rangle$ is the unique subgroup of H of size a

Proof of (II):