App. B: Review of integers.

Thm 1: Division algorithm: If m and n are integers, $n>0$, there exist unique q and r s.t. $m = nq+r$ and $0 \le r < n$.

q: quotient. r: remainder.

Def: $r, s \in \mathbb{Z}$, s is a multiple of r if $\exists$ integer k s.t. $s = rk$. In this case r is a factor of s, or r divides s. write $r|s$.

Ex: $\pm 3 | 12$, $4 | 12$

Thm 2. (i) $a|b$ & $b|c \Rightarrow a|c$

(ii) $1|a$ (iii) $a|0$ (iv) $c|a$ & $c|b \Rightarrow c|(ax+by)$ for all integers x and y

(v) If $a|b$ and $c|d$, then $ac|bd$.

Def: $t \in \mathbb{Z}$ is called a common divisor of $r, s \in \mathbb{Z}$, if $t|r$ and $t|s$.

A greatest common divisor of r and s is an integer t s.t.

(i) $t|r$ and $t|s$. and (ii) $\forall u \in \mathbb{Z}$, if $u|r$ and $u|s$, then $u|t$.

Thm 3: Any 2 nonzero integers r and s have a unique positive greatest common divisor t.

Moreover t is equal to a "linear combination" of r and s:

$$t = kr + ls \quad \text{for some integers } k \text{ and } l.$$

Def: $r, s \in \mathbb{Z}$ are said to be relatively prime if they have no common divisors except ± 1.

Thm 4: r and s are relatively prime iff $\exists\, k, l \in \mathbb{Z}$ s.t. $kr + ls = 1$.

Thm 5: If r and s are relatively prime, and $r|st$, then $r|t$.

Def: If an integer m has factors not equal to ± 1, we say that m is a composite. If $m \neq 1$ is not a composite, we call it a prime.

Thm: If $m, n \in \mathbb{Z}$. $p \mid mn$, then either $p \mid m$ or $p \mid n$.

Thm: Every positive integer $m > 1$ can be written, uniquely, as a product of primes.

Def: least common multiple of two integers r and s: a positive integer m s.t. (i) $r \mid m$ and $s \mid m$ (ii) If $r \mid x$ and $s \mid x$, then $m \mid x$.

Thm: every pair of integers r and s has a unique least common multiple. denoted by $lcm(r, s)$.

Thm: (i) $gcd(a,b) = 1 \Rightarrow lcm(a,b) = ab$

(ii) $lcm(a,b) = ab \Rightarrow gcd(a,b) = 1$.

(iii) $lcm(a,b) = \frac{ab}{gcd(a,b)}$

(iv) $lcm(a, ab) = ab$.

Chap 11: cyclic groups

$G=\{a^n; n\in\mathbb{Z}\}$ $\quad |G|=\text{ord}(a)$.

$\text{ord}(a)=k \Leftrightarrow |\langle a\rangle|=k \Leftrightarrow \langle a\rangle\cong\mathbb{Z}_k$

$\text{ord}(a)=\infty \Leftrightarrow |\langle a\rangle|=\infty \Leftrightarrow \langle a\rangle\cong\mathbb{Z}$.

Thm: Every subgroup of a cyclic group is cyclic.

Pf: $H<\underset{\text{cyclic}}{G}=\langle a\rangle$. Let m be the smallest positive integer s.t. $a^m\in H$. We will show that $\forall x\in H$, $x=(a^m)^k$ for some $k\in\mathbb{Z}$. so that $H=\langle a^m\rangle$.

write $x=a^l$ $\quad l=k\cdot m+r$ $\quad 0\le r<m-1 \Rightarrow x=a^{km+r}=(a^m)^k\cdot a^r$

$x\in H, a^m\in H \Rightarrow a^r\in H \Rightarrow r=0$. because m is the smallest positive integer s.t. $a^m\in H$

$\Rightarrow x=(a^m)^k$

Ex: A.1: $\langle 6\rangle=\{\bar{0},\bar{6},\bar{12},\overline{18}=\bar{2},\bar{8},\overline{14},\overline{20}=\bar{4},\overline{10}\}$

$|\langle 6\rangle|=\text{ord}(\bar{6})=\frac{\text{lcm}(6,16)}{6}=\frac{48}{6}=8$.

B.1: $G=\langle a\rangle$, $|G|=n \Rightarrow \text{ord}(a)=n$.

$\text{ord}(a)=n \Rightarrow \{e,a,a^2,\cdots,a^{n-1}\}=G \Rightarrow G=\langle a\rangle$ is cyclic.

C.1: $\text{ord}(a^r)=\frac{\text{lcm}(r,n)}{r}=\frac{rn}{\gcd(r,n)r}=\frac{n}{\gcd(r,n)}=n \Leftrightarrow \gcd(r,n)=1$.

Directly: a^r is a generator of $\langle a\rangle \Leftrightarrow \text{ord}(a^r)=n$.

If $\gcd(r,n)>1$ then $(a^r)^{\frac{n}{q}}=(a^n)^{\frac{r}{q}}=e \Rightarrow \text{ord}(a^r)\le\frac{n}{q}<n$. ($q=\gcd(r,n)$)

C.4: $C_m=\{x\in\langle a\rangle; x^m=e\}$ is a cyclic group $\Rightarrow C_m=\langle a^k\rangle$

$a^k\in C_m \Rightarrow \text{ord}(a^k)\le m \Rightarrow |C_m|\le m$. $\Rightarrow |C_m|=m$.

On the other hand, $\exists\, y\in G$, s.t. $\text{ord}(y)=m \Rightarrow \langle y\rangle\le C_m \Rightarrow |C_m|\ge|\langle y\rangle|=m$

C5 $\text{ord}(x)=m \Rightarrow \langle x\rangle = \{e, x, \cdots, x^{m-1}\} \subseteq C_m \Rightarrow \langle x\rangle = C_m$

$\langle x\rangle = C_m \Rightarrow \text{ord}(x)=m$

C7: $\text{ord}(a^r) = \frac{\text{lcm}(r,n)}{r} = \frac{\text{lcm}(r,mk)}{r} = m \Leftrightarrow \text{lcm}(r,mk) = mr \Leftrightarrow \gcd(r,mk)=k$

$\frac{r\cdot mk}{\gcd(r,mk)}$ (= lcm(r,mk)) ; $\Uparrow$ $r=kl$ with $\gcd(l,m)=1$

C8: $c^r = a^{kr}$ is a generator of $\langle a\rangle \Leftrightarrow \gcd(kr, n)=1 \Leftrightarrow \gcd(r,n)=1$

a^k is a generator $\Rightarrow (k,n)=1$; $(k,n)=1$

D6: $|\langle a\rangle| = mn \Rightarrow |\langle a^m\rangle| = n \Rightarrow \text{ord}(a^m)=n \Leftrightarrow \langle a^m\rangle = C_n$

Suppose H is a sbgp. of order n. then H is a cyclic gp. of order n

$\Rightarrow H = \langle a^r\rangle$ with $\text{ord}(a^r)=n \Leftrightarrow a^r$ is a generator of C_n

$\Rightarrow \langle a^r\rangle = C_n$