

Selected memoirs from Corey's troubled mind

Pinky, from Pinky and the Brain

February 3, 2008



Hi kids! This is Pinky, from Pinky and the Brain. I'm taking a break from my nightly activities of helping my friend Brain take over the world. I listened in on Corey's lecture and felt that I needed to write this document to help you all understand what was going through Corey's mind. I've illustrated with my fingers the size of his mind. So here it is.

Theorem 0.1 (The fundamental theorem of cyclic groups) *Let $G = \langle a \rangle$ be a cyclic group, and let H be a subgroup of G .*

- 1. The subgroup H is cyclic. Unless $H = \langle e \rangle$, we have $H = \langle a^t \rangle$, where t is the smallest element of the set $\{k \in \mathbb{N} \mid a^k \in H\}$.*
- 2. Suppose $|a| = n < \infty$. The order of H divides n .*
- 3. Let k be any positive divisor of n . Then there exists a unique subgroup of order k , namely, $K = \langle a^{n/k} \rangle$.*

Proof. We prove assertion (1). Suppose there exists a nonidentity element $b \in H$. Since G is cyclic, we may write $b = a^\ell$ for some integer ℓ . Since H is a subgroup, we know that $a^{-\ell} \in H$ as well, so the set $\{k \in \mathbb{N} \mid a^k \in H\}$ is nonempty, thus, it has a smallest element t .

Now we note that by closure $\langle a^t \rangle \subseteq H$. To prove the other containment, let $b = a^k \in H$. Then we divide t into k and use the division algorithm to find integers q and r with $k = tq + r$, with $0 \leq r < t$. Then $a^k = a^{tq+r} = (a^t)^q a^r$. We multiply on the left by

$(a^t)^{-q}$ to conclude that $(a^t)^{-q}a^k = a^r \in H$ since both of $(a^t)^{-q}$ and a^k are in H . But the existence of r contradicts the minimality of t unless $r = 0$. So $a^k = (a^t)^q \in \langle a^t \rangle$, and so $H \subseteq \langle a^t \rangle$.

Next we prove assertion (2). Express $H = \langle a^t \rangle$ as above, and divide t into n to get integers q and r as above, with $n = qt + r$, with $0 \leq r < t$. Now we have $a^n = a^{qt+r} = a^{qt}a^r$. But $|a| = n$, so $a^{qt}a^r = e$, and it follows that since $a^{qt} \in H$, we have $a^r \in H$. Again, the minimality of t forces us to conclude $r = 0$. So $n = qt$.

Now we compute the order of H , which by a previous result, $|H| = |\langle a^t \rangle| = |a^t|$. Suppose $|a^t| = m$. Notice that $(a^t)^q = e$, so since the order is the smallest such number that satisfies this, we have $m \leq q$. But if k is an integer so that $0 < k < q$, then $tk < tq = n$, and so $a^{tk} \neq e$. So we conclude that the order of this subgroup is q , which we note already divides n .

Now we prove the final assertion. Let k be a positive divisor of n , and as above, we express $H = \langle a^t \rangle$ be a subgroup of order k , where t is the smallest element of the set $\{k \in \mathbb{N} | a^k \in H\}$. Then the subgroup $K = \langle a^{n/k} \rangle$ has order k since $\frac{n}{k}$ is a divisor of n , and by a previous result,

$$|\langle a^{n/k} \rangle| = \frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{n/k} = k.$$

We complete the proof by showing that $K = H = \langle a^t \rangle$. We showed above that $n = tq$, where $q = k$ is the order of a^t . Then $\gcd(t, n) = t$, and $\gcd(\frac{n}{k}, n) = \frac{n}{k}$. So

$$k = |\langle a^{n/k} \rangle| = |a^t| = \frac{n}{\gcd(n, t)} = \frac{n}{t}.$$

Now we compare the far left and right to see that $t = n/k$, completing the proof. □