Math 332 HW 3

12.14. The elements of $\langle (13), \langle (1234) \rangle \rangle$ are

$$(), \ (24), \ (12)(34), \ (1234), \ (13), \ (13)(24), \ (1432), \ (14)(23)$$

12.23 For $n \geq 3$, $\text{center}(S_n) = \{()\}$.

Pf/ Let $\sigma \in S_n \setminus \{()\}$. Then $\exists\, i \in \{1, \ldots, n\}$ s.t. $\sigma(i) \neq i$. Since $n \geq 3$, $\exists\, k \in \{1, \ldots, n\} \setminus \{i, \sigma(i)\}$. Consider the transposition $\tau = (\sigma(i), k)$. Then $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i)$ and $(\tau \circ \sigma)(i) = \tau(\sigma(i)) = k \neq \sigma(i)$. $\square$

↑ Since τ fixes i.

13.5 $\varphi : G \to G'$, homo.

(a) $\ker(\varphi)$ is a subgroup of G.

Pf/ Lemma 13.3 shows $\varphi(e_G) = e_{G'}$. So $e_G \in \ker(\varphi)$.

Now suppose $a, b \in \ker(a)$. Then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) \overset{\text{Lemma 13.3}}{=} \varphi(a)\varphi(b)^{-1} = e_G, e_{G'}^{-1} = e_{G'}$$

$\Rightarrow ab^{-1} \in \ker(\varphi)$. (One could also just show $\ker(\varphi)$ is closed under multiplication and inversion separately.) $\square$

(b) $\operatorname{im}(\varphi)$ is a subgroup of G'.

Pf/ Since $\varphi(e_G) = e_{G'}$, $e_{G'} \in \operatorname{im}(\varphi)$. Let $\varphi(a) = a'$, $\varphi(b) = b'$ be arbitrary elements of $\operatorname{im}(\varphi)$. Then $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = a'(b')^{-1}$ $\in \operatorname{im}(\varphi)$. $\square$

(c) Let $H < G'$. Then $\varphi^{-1}(H)$ is a subgroup of G.

Pf/ Since $e_{G'} \in H$ and $\varphi(e_G) = e_{G'}$, we have $e_G \in \varphi^{-1}(H)$. Let $a, b \in \varphi^{-1}(H)$. Then $\varphi(a), \varphi(b) \in H \Rightarrow \varphi(ab^{-1}) =$ $\varphi(a)\varphi(b)^{-1} \in H \Rightarrow ab^{-1} \in \varphi^{-1}(H)$. $\square$

13.7 $\phi : G \to G'$ is injective iff $\ker(\phi) = \{e_G\}$.

Pf/ ($\Rightarrow$) Suppose ϕ is injective. We know $\phi(e_G) = e_{G'}$ by Lemma 13.3. So $\{e_G\} \subseteq \ker(\phi)$. Suppose $a \in \ker(\phi)$. Then $\phi(a) = \phi(e_G) = e_{G'}$.

Hence, by injectivity, $a = e_G$. So $\{e_G\} = \ker(\phi)$.

($\Leftarrow$) Now suppose $\ker(\phi) = \{e_G\}$ and $\phi(a) = \phi(b)$ for some $a, b \in G$. Then $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e_{G'} \Rightarrow ab^{-1} \in \ker(\phi)$

$\Rightarrow ab^{-1} = e_G \Rightarrow a = b$. So ϕ is injective. □

1. $H < G$, $g \in G$, $|g| = n$. Suppose $g^m \in H$ and $\gcd(m,n) = 1$. Show $g \in H$

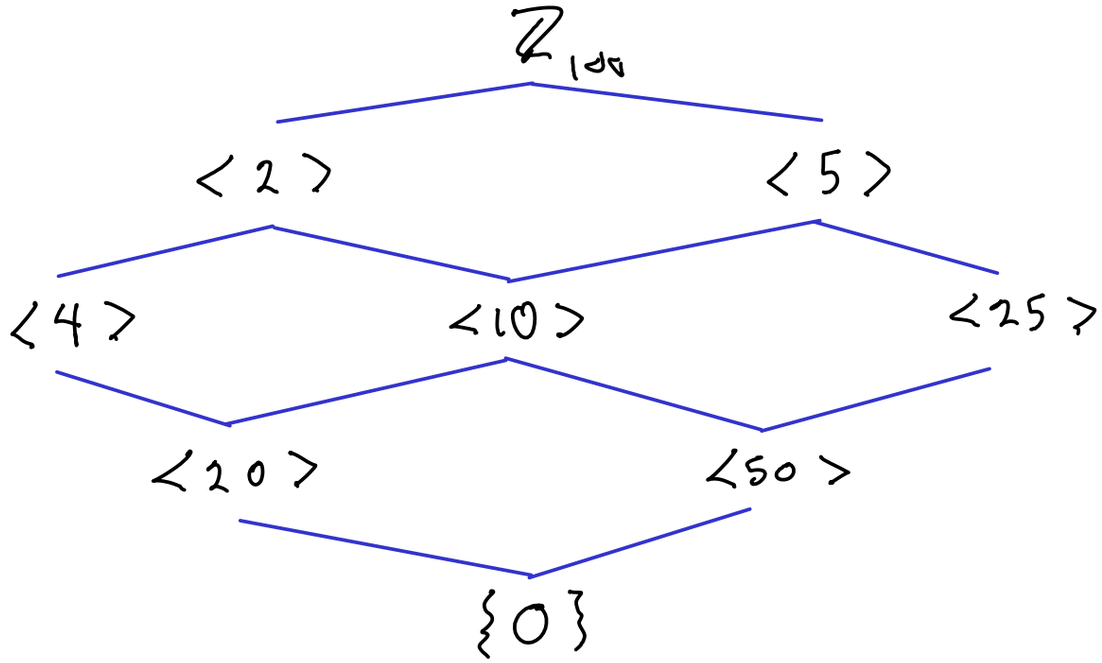
Pf/ $\gcd(m,n) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ s.t. $am + bn = 1$ (Euclidean algorithm)

$$\Rightarrow g = g^{am+bn} = (g^m)^a (g^n)^b = (g^m)^a \in H$$

Since $g^n = 1$ // since H is closed under multiplication and $g^m \in H$ □

Alternative proof:
We seen in class that $\langle g^m \rangle = \langle g^{\gcd(m,n)} \rangle$. Thus, $\langle g^m \rangle = \langle g \rangle$, which implies $g \in \langle g^m \rangle < H$. □

2.



3. $$|35| = \frac{100}{\gcd(35,100)} = \frac{100}{5} = 20.$$

4. (123) and (45678) are both even permutations (odd length). Hence, so is $(123)(45678)$. The order of this element is the lcm of the orders of (123) and (45678), i.e. the lcm of 3 and 5, i.e. 15.

5. What is the maximum order of an element of A_{10}?

Solution / Writing an element of A_{10} as a product of disjoint cycles, its order is the lcm of those cycles. There are 42 partitions of 10. Taking the lcm of their sizes gives a maximum of 30, achieved at $(1,2)(3,4,5)(6,7,8,9,10)$, for instance. But this element is not even. The next largest lcm is $\boxed{21}$, achieved at $(1,2,3)(4,5,6,7,8,9,10) \in A_{10}$, for instance. □

6. Conjecture a necessary and sufficient condition that $(1,k)$ and $(1,2,\dots,n)$ generate S_n.

Solution / $\gcd(k-1,n) = 1$. □

7. G a group with exactly 1 non-trivial proper subgroup $\Rightarrow$ G cyclic of order p^2 for some prime p.

Pf/ Let $H < G$ be the unique nontrivial proper subgroup and pick $a \in H \setminus \{1\}$. Since $\langle a \rangle$ is a nontrivial, proper subgroup

of G, we have $H = \langle a \rangle$. Say $|a| = p$. We know that if $d \mid p$, then $\langle a \rangle$ has a subgroup of order d, namely, $\langle a^{p/d} \rangle$. Hence, p must be prime (otherwise there are additional proper subgroups of of G).

Now take $b \in G \sim H$. Then $\langle b \rangle$ is a nontrivial subgroup of G not equal to H. Hence, $\langle b \rangle = G$; so G is cyclic.

There is exactly one subgroup of $\langle b \rangle$ for each divisor divisor of $|b|$: if $d \mid b$, the subgroup is $\langle b^{|b|/d} \rangle$. Since $\langle b \rangle = G$, this says that besides 1 and $|b|$, the number $|b|$ has only one other divisor. Since $\langle a \rangle < \langle b \rangle$ and $|a| = p$, we have $a = b^{|b|/p}$. So $p \mid |b|$. It follows that $|b| = p^2$. ∎