Name: Adam Frank **October 2, 2020**

Math 637: Exam 1

1. ()
Let G be a group. Prove that if $a \in G$ is the only element of order 2 then $a \in Z(G)$.

Proof. Let $b \in G$, then

$$\begin{aligned}(bab^{-1})^2 &= bab^{-1}bab^{-1} \\ &= ba^2b^{-1} \\ &= bb^{-1} \\ &= \mathbb{1}\end{aligned}$$

Therefore $bab^{-1} = a$ or $bab^{-1} = \mathbb{1}$. The latter implies $a = \mathbb{1}$ so we must have $bab^{-1} = a$ and therefore $ba = ab$ so $a \in Z(G)$.

□

2. ()
Let $|a|$ and show that $C_G(a) = C_G(a^3)$.

Proof. One direction is trivial: If $b \in C_G(a)$ then $ba^3 = a^3b$ by three operations of "swapparoo".

Now suppose $b \in C_G(a^3)$ so that $ba^3 = a^3b$. Then since $|a| = 5$ we have $b = a^3ba^2$. From this we can derive

$$\begin{aligned}ab &= a(a^3ba^2) \\ &= a^4(a^3ba^2)a^2 \\ &= a^2ba^4 \\ &= a^2(a^3ba^2)a^4 \\ &= ab\end{aligned}$$

□

3. ()
Prove that no group can have exactly two elements of order 2.

Proof. Suppose $a \neq b \in G$ each have order 2. Then we show that also ab has order 2. For $(ab)^2 = abab = \mathbb{1}$ if and only if $ab = a^{-1}b^{-1} = ab$. □

4. ()
Let p be a prime and $Z = \{z \in \mathbb{C} | z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$. For each $k \in \mathbb{Z}^+$ define $H_k = \{z \in \mathbb{Z} | z^{p^k} = 1\}$. Prove that $H_k \leq H_m$ if and only if $k \leq m$.

Proof. Suppose $H_k \leq H_m$. First note that $e^{2i\pi/p^k} \in H_k$ and if $z \in H_k$ then there exists a positive integer x such that $(e^{2i\pi/p^k})^x = z$. Likewise $e^{2i\pi/p^m} \in H_m$ and if $z \in H_m$ then there exists a positive integer x such that $(e^{2i\pi/p^m})^x = z$. Now by the subgroup relation $e^{2i\pi/p^k} \in H_m$ and therefore there is some positive integer x such that

$$e^{2i\pi/p^k} = (e^{2i\pi/p^m})^x$$

$$= e^{2i\pi x/p^m}$$

Since these complex numbers in polar form are expressed with arguments each less than 2π we can infer that

$$\frac{1}{p^k} = \frac{x}{p^m}$$

and therefore p^{m-k} is a positive integer, hence $m - k \geq 0$ and so $m \geq k$.

Conversely, suppose that $m \geq k$. Certainly the subset relation holds since $(e^{2i\pi/p^k})^{p^m} = (e^{2i\pi})^{p^{m-k}}$ and since $m - k$ is a non-negative integer, we have $(e^{2i\pi})^{p^{m-k}} = 1$. Now let $a, b \in H_k$ so that there exist poisitive integers x, y such that $a = e^{2i\pi x/p^k}$ and $b = e^{2i\pi y/p^k}$. Then since

$$ab^{-1} = e^{2i\pi(x-y)/p^k}$$

and since $x - y$ is an integer, then $(ab^{-1})^{p^k} = 1$. Hence $ab^{-1} \in H_k$ and therefore H_k is a subgroup of H_m. □

5. ()
Let Z_n be a cyclic group of order n and for each $a \in \mathbb{Z}$ let

$$\sigma_a : Z_n \to Z_n$$

by $\sigma_a(x) = x^a$. Prove that σ_a is an automorphism if and only if $(a, n) = 1$.

Proof. Suppose σ_a is an automorphism and let z generate the group Z_n. Then $\sigma_a(z)$ must also have order n. Hence n is the minimal natural number such that $z^{an} = \mathbb{1}$. □