Name: Adam Frank **October 4, 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

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

   Since there is only one element of order 2, either $bab^{-1} = a$ 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 $|a| = 5$ 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".[1]

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

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

   □

[1] Of course "swaparoo" means the old $ab = ba$.

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

   Proof. Suppose $a \neq b \in G$ each have order 2. Note in particular that this entails $a^{-1} = a$ and $b^{-1} = b$. Then we show that also ab has order 2. This follows since $(ab)^2 = abab = \mathbb{1}$ holds if and only if $ab = a^{-1}b^{-1} = ab$. The later of course is a tautology. $\square$

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 non-negative 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 non-negative 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 non-negative integer x such that

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

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

   In particular we can choose $0 \leq 2\pi x/p^m < 2\pi$. 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 non-negative 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. $\square$

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. Let $d = (a, n)$ and let z generate Z_n. First suppose $d > 1$ for the contrapositive. Let $n = xd$ and $a = yd$. Note in particular that $1 < x < n$ so that $z^x \neq \mathbb{1}$. Now we have

$$\sigma_a(z^x) = z^{ax} = z^{ydx} = z^{yn} = \mathbb{1}$$

This shows that σ_a is not injective, since $\sigma_a(\mathbb{1}) = \mathbb{1} = \sigma_a(z^x)$. This concludes one direction of the proof.

Now suppose that $d = 1$. We will see that the map is injective, so suppose that $\sigma_a(z^p) = \sigma_a(z^q)$ so that therefore

$$z^{ap} = z^{aq}$$

Hence $ap \equiv aq \mod n$, and because $d = 1$ we can infer that $p \equiv q \mod n$. But this entails that $z^p = z^q$.

Now since Z_n is finite and $\sigma_a : Z_n \to Z_n$ then surjectivity follows from injectivity. All that remains is to see that the map is a homomorphism. But $\sigma_a(z^i z^j) = z^{(i+j)a} = z^{ia} z^{ij} = \sigma_a(z^i)\sigma_a(z^j)$.

(In case the principle used above needs justification: We know that $ap \equiv aq \mod n$ entails $p \equiv q \mod n$ because we can multiply both sides of the first equivalence by the inverse of a. This is guaranteed to exist by Bezout's identity $ax + ny = 1$, which makes x the multiplicative inverse of a.)

□

6. ()
   Prove that no group is the union of two proper subgroups.

   Proof. Suppose $G = A \cup B$ where $A, B < G$. If $A \leq B$ then $A \cup B = B < G$, so this is impossible, and there must be some $a \in A$ where $a \notin G \setminus B$. By a symmetric consideration, there must be some $b \in B$ where $b \notin G \setminus A$. Now either $ab \in A$ or $ab \in B$. Without loss of generality suppose $ab \in A$. But then $a^{-1} \in A$ and hence $a^{-1}ab = b \in A$, a contradiction. $\lightning$ □

7. ()
   Let G be a finite group with more than one element. Show that G has an element of prime order.

   Proof. There must exist an element of order greater than 1, call it $g \in G$. Now consider the group generated by g, which is $\langle g \rangle$. This is a cyclic group and therefore if d is any divisor of $|g|$ then there is an element of order d (namely, $g^{|g|/d}$, due to theorem 7 of section 2.3 of Dummit and Foote). In particular there must be some prime divisor of $|g|$, which entails the existence of an element of prime order. □

8. ()
   Suppose G is a finite abelian group and G has no element of order 2. Show that $x \mapsto x^2$ is an automorphism.

   Proof. We show that the map, call it φ, is injective. If $\varphi(x) = \varphi(y) = x^2 = y^2$ then $\mathbb{1} = x^{-2}y^2 = (x^{-1}y)^2$ since G is abelian. But since $x^{-1}y$ can't have order 2, it must have order 1 and be the identity. Then $\mathbb{1} = x^{-1}y$ and therefore $x = y$.

   Since φ is a map from G to G, and since G is finite, then injectivity implies surjectivity. All that remains is to show that φ is a homomorphism. But this follows from abelianness:

$$\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$$

   "Abelianness" ... "abelianity" ... "abelianism". You know what I meant. □