Cavallaro, Jeffery
Math 221a
Homework #3

1.3.11

Let G be a group and $a, b \in G$. Prove:

1). $|a| = |a^{-1}|$

Assume $x \in \langle a \rangle$
$\exists\, n \in \mathbb{Z}, x = a^n$
$x = (a^{-1})^{-n}, -n \in \mathbb{Z}$
$x \in \langle a^{-1} \rangle$
$\langle a \rangle \subseteq \langle a^{-1} \rangle$

Assume $x \in \langle a^{-1} \rangle$
$\exists\, m \in \mathbb{Z}, x = (a^{-1})^m$
$x = a^{-m}, -m \in \mathbb{Z}$
$x \in \langle a \rangle$
$\langle a^{-1} \rangle \subseteq \langle a \rangle$

$\langle a \rangle = \langle a^{-1} \rangle$
$\therefore |a| = |a^{-1}|$

2). $|ab| = |ba|$

If $a = b = e$ then $|ab| = |ba| = 1$, so AWLOG that $a \neq e$ or $b \neq e$

Assume $\langle ab \rangle$ is finite
Let $|ab| = n$
$(ab)^n = e$
$b(ab)^n a = bea$
$(ba)^{n+1} = ba$
$(ba)^n = e$
$|ba| \leq n$
$|ba| \leq |ab|$ and $\langle ba \rangle$ is finite

Assume $\langle ba \rangle$ is finite
Let $|ba| = m$
$(ba)^m = e$
$a(ba)^m b = aeb$
$(ab)^{m+1} = ab$
$(ab)^m = e$
$|ab| \leq m$
$|ab| \leq |ba|$ and $\langle ab \rangle$ is finite

$\therefore \langle ab \rangle$ finite $\iff \langle ba \rangle$ finite, and so if $\langle ab \rangle$ is finite then so is $\langle ba \rangle$, and $|ab| = |ba|$.

By the CP, $\langle ab \rangle$ infinite $\iff \langle ba \rangle$ infinite, and all infinite cyclic groups are isomorphic to $\mathbb{Z}$ (and each other). So if $\langle ab \rangle$ is infinite then so is $\langle ab \rangle$, and $|ab| = |ba| = \aleph_0$.

$\therefore |ab| = |ba|$

3). $\forall\, c \in G, |a| = |cac^{-1}|$

Assume $c \in G$

Lemma

$$\forall\, n \in \mathbb{Z}^+, (cac^{-1})^n = ca^n c^{-1}$$

Proof

Proof by induction on n:

Base: $n = 1$

$$(cac^{-1})^1 = cac^{-1} = ca^1 c^{-1}$$

Assume $(cac^{-1})^n = ca^n c^{-1}$

$(cac^{-1})^{n+1} = (cac^{-1})^n (cac^{-1}) = ca^n c^{-1} cac^{-1} = ca^n eac^{-1} = ca^n ac^{-1} = ca^{n+1} c^{-1}$

If $a = e$ then $cac^{-1} = cec^{-1} = cc^{-1} = e$, and so $|a| = |cac^{-1}| = 1$

If $c = e$ then $cac^{-1} = eae^{-1} = eae = a$, and so $|cac^{-1}| = |a|$

If $cac^{-1} = e$ then $a = c^{-1}ec = c^{-1}c = e$, and so $|a| = |cac^{-1}| = 1$

So AWLOG that $a \neq e$, $c \neq e$, and $cac^{-1} \neq e$

Assume $\langle a \rangle$ is finite
Let $|a| = n, n \in \mathbb{Z}^+$
$a^n = e$
$(cac^{-1})^n = ca^n c^{-1} = cec^{-1} = cc^{-1} = e$
$|cac^{-1}| \leq n$
$|cac^{-1}| \leq |a|$ and $\langle cac^{-1} \rangle$ is finite

Assume $\langle cac^{-1} \rangle$ is finite
Let $|cac^{-1}| = m, m \in \mathbb{Z}^+$
$(cac^{-1})^m = e$
$ca^m c^{-1} = e$
$a^m = c^{-1}ec = c^{-1}c = e$
$|a| \leq m$
$|a| \leq |cac^{-1}|$ and $\langle a \rangle$ is finite

$\therefore \langle a \rangle$ finite $\iff \langle cac^{-1} \rangle$ finite, and so if $\langle a \rangle$ is finite then so is $\langle cac^{-1} \rangle$, and $|a| = |cac^{-1}|$.

By the CP, $\langle a \rangle$ infinite $\iff$ $\langle cac^{-1} \rangle$ infinite, and all infinite cyclic groups are isomorphic to $\mathbb{Z}$ (and each other). So if $\langle a \rangle$ is infinite then so is $\langle cac^{-1} \rangle$, and $|a| = |cac^{-1}| = \aleph_0$.

$\therefore |a| = |cac^{-1}|$

1.3.2

Let G be an abelian group. Let $a, b \in G$ such that $\langle a \rangle$ and $\langle b \rangle$ are finite with $|a| = m$ and $|b| = n$.

Prove: $\exists\, c \in G, |c| = [m, n]$

Lemma

Let G be an abelian group. Let $a, b \in G$ such that $\langle a \rangle$ and $\langle b \rangle$ are finite with $|a| = m$ and $|b| = n$ such that $(m, n) = 1$.

$\exists\, c \in G, |c| = mn$

Proof

Let $c = ab \in G$
$\langle c \rangle \leq G$
$c^{rs} = (ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e^s e^r = ee = e$
So $\langle c \rangle$ is finite
Let $|c| = n$
$n \leq rs$

$c^n = e$
$(ab)^n = e$
$a^n b^n = e$
$a^n = b^{-n}$
Let $\ell = a^n = b^{-n}$
$\ell \in \langle a \rangle$ and $\ell \in \langle b \rangle$
$\langle \ell \rangle \leq \langle a \rangle$ and $\langle \ell \rangle \leq \langle b \rangle$
$|\ell| \mid r$ and $|\ell| \mid s$
ℓ is a common divisor of r and s
But $(r, s) = 1$
So $|\ell| = 1$ and thus $\ell = e$
$a^n = b^{-n} = e$
$b^n = e$
$r \mid n$ and $s \mid n$
n is a common multiple of r and s
But since $(r, s) = 1, [r, s] = rs$, and so:
$rs \leq n$

$\therefore rs = n$

$\therefore \langle c \rangle \leq G$ and $|c| = rs$

Now, let $d = (r, s)$
$[r, s] = \frac{rs}{d}$
Let $s_0 = \frac{s}{d}$
$(r, s_0) = 1$

$|a| = r$
$\left|b^d\right| = \frac{s}{(d,s)} = \frac{s}{(d,ds_0)} = \frac{s}{d} = s_0$

So by the lemma:
$\exists\, c \in G, |c| = rs_0$
But $rs_0 = \frac{rs}{d} = [r, s]$

$\therefore \exists\, c \in G, |c| = [r, s]$

1.3.3

Let G be an abelian group of order pq such that $(p, q) = 1$.

Prove: $(\exists\, a, b \in G, |a| = p$ and $|b| = q) \implies G$ is cyclic

Assume $\exists\, a, b \in G, |a| = p$ and $|b| = q$
By the lemma:
$\exists\, c \in G, |c| = pq$
$\langle c \rangle \leq G$ and $|c| = |G|$
So $\langle c \rangle = G$
$\therefore G$ is cyclic.

1.3.4

Let $\phi : G \to H$ be a homomorphism of groups.

Prove: $a \in G$ and $\phi(a)$ has finite order in $H \implies |a|$ is infinite or $|\phi(a)| \mid |a|$

Assume $a \in G$ and $\phi(a)$ has finite order in H
If $|a|$ is infinite then done, so assume $|a|$ is finite
Let $|a| = n$
$a^n = e_G$
$\phi(a^n) = \phi(a)^n$
$\phi(a^n) = \phi(e_G) = e_H$
$\phi(a)^n = e_H$
So $|\phi(a)| \mid n$
$\therefore |\phi(a)| \mid |a|$

1.3.5

Let $G = GL_2(\mathbb{Q})$.

1). Let $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Show $|a| = 4$

$$a^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$a^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

2). Let $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Show $|b| = 3$

$$b^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$b^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

3). Show $|ab| = \aleph_0$

$$ab = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Claim: $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

case 1: $n > 0$

Proof by induction on n

Base: $n = 1$

$$(ab)^1 = ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Assume $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$$(ab)^{n+1} = (ab)^n(ab) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

case 2: $n = 0$

$$(ab)^0 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

case 3: $n < 0$

Claim: $\forall\, n > 0, [(ab)^n]^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

Let $m = -n > 0$

$(ab)^n = (ab)^{-m} = [(ab)^m]^{-1} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Let $A = \{(ab)^n \mid n \in \mathbb{N}\}$
Define $\phi : \mathbb{N} \to A$ by $\phi(n) = (ab)^n$
Let $\phi^{-1} : A \to N$ be defined by $\phi^{-1}\left((ab)^n\right) = n$
$(\phi\phi^{-1})\left((ab)^n\right) = \phi(n) = (ab)^n$
$(\phi^{-1}\phi)(n) = \phi^{-1}\left((ab)^n\right) = n$
So ϕ is invertible, and thus bijective
$\phi(n+m) = (ab)^{n+m} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$
$\phi(n)\phi(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$
$\phi(n+m) = \phi(n)\phi(m)$
So ϕ is a homomorphism, and thus an isomorphism
So A has infinite order
But $A \subset \langle ab \rangle$
$\therefore ab$ has infinite order.

4). Show that $Z_2 \oplus \mathbb{Z}$ has elements a and b of infinite order such that $a + b$ has finite order.

Let $a = (0, 1)$ and $b = (0, -1)$

Clearly, a and b have infinite order:

$$na = (0, n)$$

$$nb = (0, -n)$$

But $a + b = (0, 1) + (0, -1) = (0, 0) = e$, and $\langle e \rangle$ is finite with order 1.

1.3.8

Prove: A group that has only a finite number of subgroups must be finite.

Assume that G is a group with only a finite number of subgroups
ABC: $\exists\, a \in G$ such that a has infinite order
$\langle a \rangle \simeq \mathbb{Z}$, which has an infinite number of subgroups
So $\langle a \rangle$, and thus G, have an infinite number of subgroups

CONTRADICTION!
Thus G is a union of a finite number of finite subgroups
$\therefore G$ is finite.

1.3.9

Let G be an abelian group and define $T = \{a \in G \mid a \text{ has finite order}\}$.

Prove: $T \leq G$

$|e| = 1$, so $e \in T$ and $T \neq \emptyset$

Assume $a, b \in T$
By closure, $ab \in G$
Let $|a| = r$ and $|b| = s$
$(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e^s e^r = ee = e$
Thus, ab has finite order
$ab \in T$
$\therefore T$ is closed.

Assume $a \in T$
$|a| = |a^{-1}|$
a^{-1} has finite order
$a^{-1} \in T$
$\therefore T$ has inverses.

$\therefore T \leq G$