Math 4550
HW 1
Solutions

①

$\mathbb{Z}_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

inverse of $\bar{0}$ is $\bar{0}$
inverse of $\bar{1}$ is $\bar{1}$

---

②

$\mathbb{Z}_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

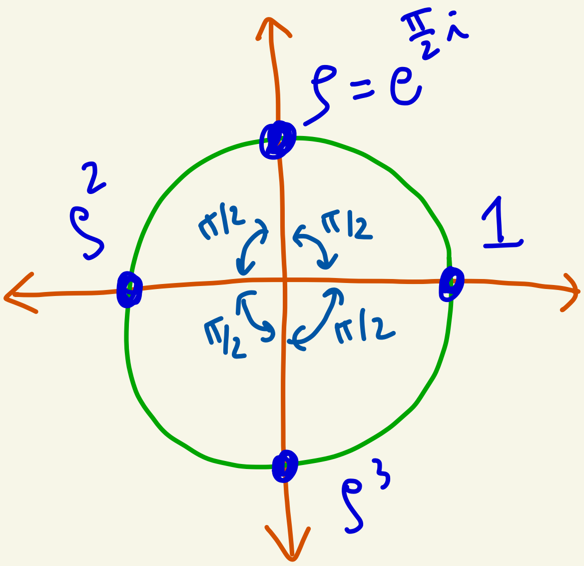
inverse of $\bar{0}$ is $\bar{0}$
inverse of $\bar{1}$ is $\bar{3}$
inverse of $\bar{2}$ is $\bar{2}$
inverse of $\bar{3}$ is $\bar{1}$

---

③ $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

element	inverse	
$\bar{0}$	$\bar{0}$	← because $\bar{0}+\bar{0}=\bar{0}$
$\bar{1}$	$\bar{5}$	← because $\bar{1}+\bar{5}=\bar{6}=\bar{0}$
$\bar{2}$	$\bar{4}$	← because $\bar{2}+\bar{4}=\bar{6}=\bar{0}$
$\bar{3}$	$\bar{3}$	← because $\bar{3}+\bar{3}=\bar{6}=\bar{0}$
$\bar{4}$	$\bar{2}$	← because $\bar{4}+\bar{2}=\bar{6}=\bar{0}$
5	$\bar{1}$	← because $\bar{5}+\bar{1}=\bar{6}=\bar{0}$

④ $U_4 = \{1, \rho, \rho^2, \rho^3\}$ where $\rho = e^{\frac{2\pi i}{4}} = e^{\frac{\pi}{2} i}$



U_4	1	ρ	ρ^2	ρ^3
1	1	ρ	ρ^2	ρ^3
ρ	ρ	ρ^2	ρ^3	1
ρ^2	ρ^2	ρ^3	1	ρ
ρ^3	ρ^3	1	ρ	ρ^2

KEY FORMULA:

Use $\rho^4 = 1$ to calculate.

element	inverse
1	1
ρ	ρ^3
ρ^2	ρ^2
ρ^3	ρ

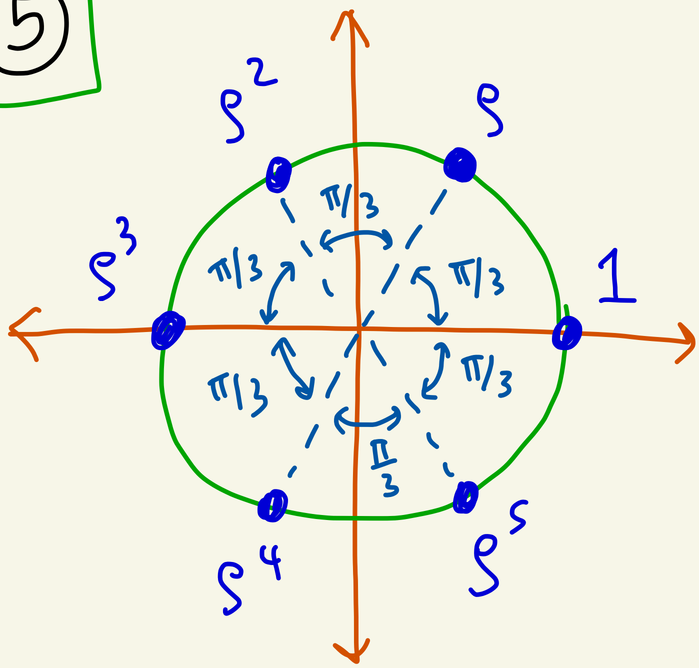
← because $1 \cdot 1 = 1$

← because $\rho \cdot \rho^3 = \rho^4 = 1$

← because $\rho^2 \cdot \rho^2 = \rho^4 = 1$

← because $\rho^3 \cdot \rho = \rho^4 = 1$

(5)



$U_6 = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$

where $\rho = e^{\frac{2\pi i}{6}} = e^{\frac{\pi}{3} i}$

KEY FORMULA:

Use $\rho^6 = 1$ to calculate

element	inverse	
1	1	because $1 \cdot 1 = 1$
ρ	ρ^5	because $\rho \cdot \rho^5 = \rho^6 = 1$
ρ^2	ρ^4	because $\rho^2 \cdot \rho^4 = \rho^6 = 1$
ρ^3	ρ^3	because $\rho^3 \cdot \rho^3 = \rho^6 = 1$
ρ^4	ρ^2	because $\rho^4 \cdot \rho^2 = \rho^6 = 1$
ρ^5	ρ	because $\rho^5 \cdot \rho = \rho^6 = 1$

⑥ $D_6 = \{1, r, r^2, s, sr, sr^2\}$

Use: $r^3 = 1,\ s^2 = 1,\ r^k s = s r^{-k} = s r^{3-k}$

D_6	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

inverses:

$1^{-1} = 1$ $s^{-1} = s$

$r^{-1} = r^2$ $(sr)^{-1} = sr$

$(r^2)^{-1} = r$ $(sr^2)^{-1} = sr^2$

7 (a)

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

$\boxed{\text{Use: } r^4 = 1,\ s^2 = 1,\ r^k s = s r^{-k} = s r^{4-k}}$

(b) $r s r^3 = s r^{-1} r^3 = s r^2$

$(sr^3)(sr^2) = s r^3 s r^2 = s s r^{-3} r^2 = s^2 r^{-1} = 1 r^3 = r^3$

$\boxed{r^{-1} = r^4 r^{-1} = r^3 \text{ since } r^4 = 1}$

$r^2 r^3 s r s r^{-2} = r^5 s r s r^{-2} = r s r s r^{-2}$

$\boxed{r^4 = 1 \to r^5 = r^4 r = r}$

$= s r^{-1} r s r^{-2} = s 1 s r^{-2}$

$= s^2 r^{-2} = 1 r^{-2} = r^{-2} = r^4 r^{-2} = r^2$

(c) $r \cdot r^3 = r^4 = 1$ thus $r^{-1} = r^3$

$r^2 \cdot r^2 = r^4 = 1$ thus $(r^2)^{-1} = r^2$

$(sr)(sr) = s r s r = s s r^{-1} r = s^2 \cdot 1 = 1 \cdot 1 = 1$

thus $(sr)^{-1} = sr$

$(sr^2)(sr^2) = s r^2 s r^2 = s s r^{-2} r^2 = s^2 \cdot 1 = 1 \cdot 1 = 1$

thus $(sr^2)^{-1} = sr^2$

---

8 (a) $A = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}$ $\quad B = \begin{pmatrix} 1 & 0 \\ 1/2 & 5 \end{pmatrix}$

$$\det(A) = 1\cdot 1 - (-1)(2) = 1 + 2 = 3 \neq 0$$
$$\det(B) = 1\cdot 5 - 0\cdot \tfrac{1}{2} = 5 \neq 0$$

Thus, $A, B \in GL(2,\mathbb{R})$

To show that A and B are in $GL(2,\mathbb{R})$ you show they have non-zero determinant

Now we calculate A^{-1}, B^{-1}, and AB.

We need this formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Thus,

$$A^{-1} = \frac{1}{1\cdot 1-(-1)(2)}\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 1/3 & 1/3 \\ -2/3 & 1/3 \end{pmatrix}$$

$$B^{-1} = \frac{1}{1\cdot 5 - 0\cdot\frac{1}{2}}\begin{pmatrix} 5 & 0 \\ -1/2 & 1 \end{pmatrix} = \frac{2}{9}\begin{pmatrix} 5 & 0 \\ -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} 10/9 & 0 \\ -1/9 & 2/9 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1/2 & 5 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 - 1\cdot\frac{1}{2} & 1\cdot 0 - 1\cdot 5 \\ 2\cdot 1 + 1\cdot\frac{1}{2} & 2\cdot 0 + 1\cdot 5 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -5 \\ \frac{3}{2} & 5 \end{pmatrix}$$

8 (b) $A = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$ $B = \begin{pmatrix} -1 & 1 \\ -1 & 2 \end{pmatrix}$

$\det(A) = 5 \cdot 3 - 0 \cdot 0 = 15 \neq 0$

$\det(B) = (-1)(2) - (1)(-1) = -1 \neq 0$

Thus, $A, B \in GL(2, \mathbb{R})$

To show that A and B are in $GL(2,\mathbb{R})$ you show they have non-zero determinant

Now we calculate A^{-1}, B^{-1}, and AB.

We need this formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Thus,

$$A^{-1} = \frac{1}{5 \cdot 3 - 0 \cdot 0} \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} = \frac{1}{15} \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1/5 & 0 \\ 0 & 1/3 \end{pmatrix}$$

$$B^{-1} = \frac{1}{(-1)(2)-(1)(-1)} \begin{pmatrix} 2 & -1 \\ 1 & -1 \end{pmatrix} = \frac{1}{-1} \begin{pmatrix} 2 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -1 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -5+0 & 5+0 \\ 0-3 & 0+6 \end{pmatrix} = \begin{pmatrix} -5 & 5 \\ -3 & 6 \end{pmatrix}$$

9 We know that

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

Where $r^n = 1$, $s^2 = 1$, $r^k s = sr^{-k}$.

Thus,

$$\begin{aligned}(sr^k)(sr^k) &= s r^k s r^k \\ &= s s r^{-k} r^k \\ &= s^2 \cdot 1 \\ &= 1 \cdot 1 \\ &= 1\end{aligned}$$

$r^k s = sr^{-k}$

$s^2 = 1$

To show that $x^{-1} = y$ show that $xy = 1$.

This is the definition of inverse.

Since $(sr^k)(sr^k) = 1$ we know that $(sr^k)^{-1} = sr^k$.

$\boxed{10}$

Suppose that $a*b = a*c$.
Since G is a group and $a \in G$ there exists a^{-1} in G.
Multiply $a*b = a*c$ by a^{-1} to get

$$a^{-1}*(a*b) = a^{-1}*(a*c)$$

By associativity in G we get

$$(a^{-1}*a)*b = (a^{-1}*a)*c$$

Thus,

$$e*b = e*c$$

where e is the identity of G.

So,

$$b = c.$$

$\blacksquare$

11

Our assumption is that if $x \in G$ then $x^{-1} = x$. That is, $x * x = e$.

Let's show that G is abelian.

we must show that $a * b = b * a$

Let $a, b \in G$.

By assumption we know

$$(a*b)*(a*b) = e$$

$$a * a = e$$

$$b * b = e$$

we are assuming that $x * x = e$. Plug in $x = a * b$.

$x = a$

$x = b$

to get these.

So, $a * b * a * b = e$.

Apply a on the left to get

$$\underbrace{a*(a}_{e} * b * a * b) = a * e$$

Thus,

$$b * a * b = a.$$

Apply b to the left to get

$$b*(b*a*b) = b*a.$$

e

Thus,

$$a*b = b*a.$$

∎

(12) $\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$

(a) Let's show that $\mathbb{Z}_{10}$ is not a group under multiplication.

The identity is $\bar{1}$ under multiplication.
Let's show that $\bar{2}$ has no inverse.
Try all combinations:

$$\left.\begin{aligned}
\bar{2}\cdot\bar{0} &= \bar{0} \\
\bar{2}\cdot\bar{1} &= \bar{2} \\
\bar{2}\cdot\bar{2} &= \bar{4} \\
\bar{2}\cdot\bar{3} &= \bar{6} \\
\bar{2}\cdot\bar{4} &= \bar{8} \\
\bar{2}\cdot\bar{5} &= \bar{0} \\
\bar{2}\cdot\bar{6} &= \overline{12} = \bar{2} \\
\bar{2}\cdot\bar{7} &= \overline{14} = \bar{4} \\
\bar{2}\cdot\bar{8} &= \overline{16} = \bar{6} \\
\bar{2}\cdot\bar{9} &= \overline{18} = \bar{8}
\end{aligned}\right\} \text{none of these equal } \bar{1}.$$

we are in $\mathbb{Z}_{10}$

Thus, $\bar{2}$ has no inverse under multiplication.

(b) Let $G = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ in $\mathbb{Z}_{10}$.

We will show that G is a group under multiplication.

Since we are in $\mathbb{Z}_{10}$ we know that

$$\overline{a} * (\overline{b} * \overline{c}) = (\overline{a} * \overline{b}) * \overline{c}.$$

Let's check for closure, identity, and inverses

G	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{4}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{8}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$

we are in $\mathbb{Z}_{10}$ so for example

$$\overline{6} \cdot \overline{4} = \overline{24} = \overline{4}$$

differ by $20 = 2 \cdot 10$

note:

① G is closed under multiplication

② $\overline{2} \cdot \overline{6} = \overline{2}$
$\overline{4} \cdot \overline{6} = \overline{4}$
$\overline{6} \cdot \overline{6} = \overline{6}$
$\overline{8} \cdot \overline{6} = \overline{8}$

So $\overline{6}$ is the identity under multiplication

③ $\overline{2} \cdot \overline{8} = \overline{6}$
$\overline{4} \cdot \overline{4} = \overline{6}$
$\overline{6} \cdot \overline{6} = \overline{6}$

$\overline{6}$ is identity.

Thus,
$\overline{2}^{-1} = \overline{8}$
$\overline{4}^{-1} = \overline{4}$
$\overline{8}^{-1} = \overline{2}$
$\overline{6}^{-1} = \overline{6}$

(13)

$\mathbb{Z}-\{0\} = \{\ldots, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, \ldots\}$

The identity element under multiplication is 1.

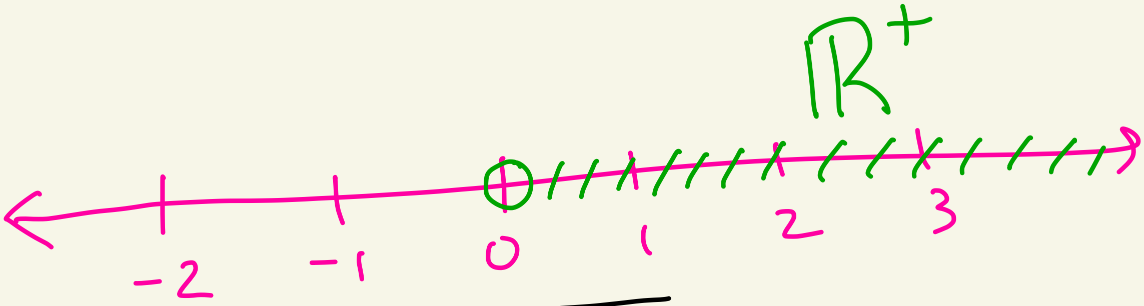
Note that 2 does not have an inverse.

For we would need $2x = 1$ for some $x \in \mathbb{Z}-\{0\}$.

But this would require $x = \frac{1}{2}$ which is not in $\mathbb{Z}-\{0\}$.

So, $\mathbb{Z}-\{0\}$ is not a group under multiplication.

(14) Let $\mathbb{R}^+$ denote the set of positive real numbers.



Consider $x * y = \sqrt{xy}$

For example, $2 * 3 = \sqrt{2 \cdot 3} = \sqrt{6}$

This operation is not associative.

For example

$$1 * (2 * 3) = \sqrt{1 \cdot (2 * 3)} = \sqrt{1 \cdot \sqrt{2 \cdot 3}}$$

$$= \sqrt{\sqrt{23}} \approx 2.45$$

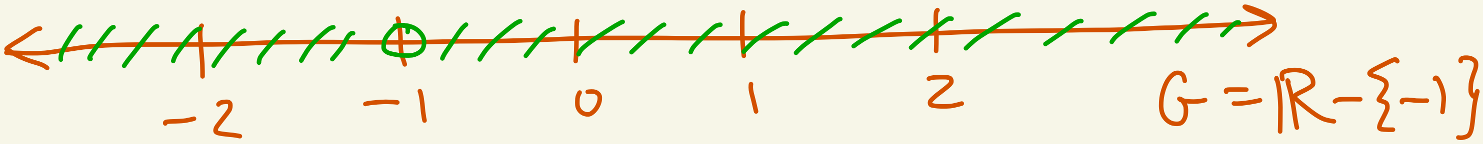
and

$$(1 * 2) * 3 = \sqrt{(1 * 2) \cdot 3} = \sqrt{\sqrt{1 \cdot 2} \cdot 3}$$

$$= \sqrt{\sqrt{2} \cdot 3} \approx 2.06$$

So, $*$ is not associative and $\mathbb{R}^+$ is not a group under $*$.

(15) Let $G = \mathbb{R} - \{-1\}$.



We will show that G is a group under the operation $a * b = a + b + ab$

(i) Suppose $a, b \in G$.

Then $a, b \in \mathbb{R}$ and $a \neq -1, b \neq -1$.

We will show that $a * b \in G$.

We have $a * b = a + b + ab$.

This is a real number in $\mathbb{R}$.

We show $a + b + ab \neq -1$.

Suppose $a + b + ab = -1$.

Then, $a + ab = -1 - b$

Thus, $a(1+b) = -(1+b)$. can divide by $1+b$ since $b \neq -1$ so $1+b \neq 0$.

Then, $a = -1$.

Contradiction.

Thus, $a * b = a + b + ab$ is in $\mathbb{R}$ but not -1.

So, $a * b \in G$.

(ii) Let $a, b, c \in G$.

Then,

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

and

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

We see that

$$a * (b * c) = (a * b) * c.$$

(iii) We will show that $e = 0$.

Heres how I got $e = 0$.
We need $e * x = x$ for all x.
This gives $e + x + ex = x$
That is $e + ex = 0$
or, $e(1 + x) = 0$ for all x.

So, $e=0$ or $1+x=0$.
Since $x \neq -1$ for all $x \in G$
we need $e=0$

Let $x \in G$.
Then,
$$0 * x = 0 + x + 0x = x$$
and
$$x * 0 = x + 0 + x0 = x$$
So, 0 is the identity element.

(iv) Let $x \in G$.
Then $x \in \mathbb{R}$ and $x \neq -1$.
We want to find an inverse y for x.
We need $x * y = 0$ ← $e=0$
So, need $x + y + xy = 0$.
That is $y + xy = -x$
or, $y(1+x) = -x$
That is, $y = \frac{-x}{1+x}$ which exists since $1+x \neq 0$ because $x \neq -1$.

Is y in G?

If it wasn't then $\frac{-x}{1+x} = -1$.

But then $-x = -1-x$ or $0=-1$ which can't happen.

So, $y \in G \leftarrow$ $y \in \mathbb{R}$ and $y \neq -1$

Let's show that $x^{-1} = \frac{-x}{1+x}$.

We have

$$\left(\frac{-x}{1+x}\right) * x = \frac{-x}{1+x} + x + \left(\frac{-x}{1+x}\right)x$$

$$= \frac{-x+x+x^2-x^2}{1+x} = \frac{0}{1+x} = 0$$

and

$$x * \left(\frac{-x}{1+x}\right) = x + \frac{-x}{1+x} + x\left(\frac{-x}{1+x}\right)$$

$$= \frac{x+x^2-x-x^2}{1+x} = \frac{0}{1+x} = 0$$

So, $x * \left(\frac{-x}{1+x}\right) = 0$ and $\left(\frac{-x}{1+x}\right) * x = 0$ where 0 is the identity. Thus, $x^{-1} = \frac{-x}{1+x}$.

By (i), (ii), (iii), (iv) we have that G is a group under $a * b = a + b + ab$ $\boxtimes$

16 Let G be an abelian group.

Let $a, b \in G$.

We will show by induction that $(a*b)^n = (a^n) * b^n$.

If $n=1$ then

$$(a*b)^1 = a*b = (a^1)*(b^1).$$

Suppose

$$(a*b)^k = (a^k)*(b^k) \qquad (*)$$

for some k.

Then,

$x^{k+1} = x^k * x^1$

$$\begin{aligned}(a*b)^{k+1} &= (a*b)^k * (a*b) \\ &= (a^k)*(b^k)*a*b \quad \text{by } (*) \\ &= (a^k)*a*(b^k)*b \quad \text{since } G \text{ is abelian} \\ &= (a^{k+1})*(b^{k+1})\end{aligned}$$

We have shown $(a*b)^{k+1} = (a^k)*(b^k)$.

By induction $(a*b)^n = (a^n)*(b^n)$ for all n.

$\blacksquare$