Homework 2 Solutions

Chapter 2

1. Which of the following operations are closed?

(a) $(\mathbb{Z}^+, -)$ is not closed since $1-2=-1 \notin \mathbb{Z}^+$.

(b) $(\mathbb{Z}\setminus\{0\}, \div)$ is not closed since $\frac{1}{2} \notin \mathbb{Z}\setminus\{0\}$.

(c) Function composition of polynomials with real coefficients is closed

(d) Multiplication of 2×2 matrices w/ integer entries is closed.

2. Which of the following binary operations are associative?

(a) Multiplication mod n is associative (see Thm 6 from class)

(b) $(\mathbb{Q}\setminus\{0\}, \div)$ is not associative since $1\div(2\div 2) = 1 \neq \frac{1}{4} = (1\div 2)\div 2$.

(c) Function composition of polynomials w/ real coeff. is associative

(d) Multiplication of 2×2 matrices w/ integer entries is associative.

3. Which of the following binary operations are commutative?

(a) $(\mathbb{Z}, -)$ is not commutative since $1-2=-1\neq 1 = 2-1$.

(b) $(\mathbb{R}\setminus\{0\}, \div)$ is not commutative since $\frac{1}{2} \neq \frac{2}{1} = 2$.

(c) Function composition of polynomials w/ real coeff. is not commutative: let $f(x)=x^2$, $g(x)=2x$. Then $(fg)(x) = 4x^2$ but $(gf)(x) = 2x^2$.

(d) Multiplication of 2×2 matrices w/ real entries is not commutative:

$$\begin{bmatrix}1&-1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\-1&1\end{bmatrix} = \begin{bmatrix}2&-1\\-1&1\end{bmatrix} \text{ but } \begin{bmatrix}1&0\\-1&1\end{bmatrix}\begin{bmatrix}1&-1\\0&1\end{bmatrix} = \begin{bmatrix}1&-1\\-1&2\end{bmatrix}.$$

2. Give an example of group elements $a + b$ s.t. $a^{-1}ba \neq b$.

Let $G = D_4$, $a = R_{90}$, $b = H$. Then $a^{-1}ba = R_{270}HR_{90} = R_{270}D = V \neq H$. (other examples are possible)

13. Translate the following multiplicative expressions to the additive counterpart:

(a) $a^2b^3 \longrightarrow 2a+3b$

(b) $a^{-2}(b^{-1}c)^2 \longrightarrow -2a + 2(-b+c)$

(c) $(ab^2)^{-3}c^2 = e \longrightarrow -3(a+2b)+2c = 0$

18. List the members of $H = \{x^2 \mid x\in D_4\}$ and $K = \{x\in D_4 \mid x^2 = e\}$.

$H = \{R_0, R_{180}\}$, $K = \{R_0, R_{180}, H, V, D, D'\}$

19. Prove that the set S of 2×2 matrices with real entries and determinant 1 is a group under matrix multiplication.

Proof Let $A, B\in S$. Then $\det(AB) = \det(A)\cdot\det(B) = 1\cdot 1 = 1$, so $AB\in S$ and the operation is closed. The operation of matrix multiplication is associative with identity $\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

If $A\in S$ is given by $A = \begin{bmatrix}a&b\\c&d\end{bmatrix}$, then $ad-bc=1$ since $A\in S$ and

$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix} = \begin{bmatrix}d&-b\\-c&a\end{bmatrix}$ has determinant $da-(-b)(-c) = ad-bc = 1$.

Thus, $A^{-1}\in S$ and S is a group. $\blacksquare$

25. Prove that a group G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ $\forall a,b \in G$.

Proof Assume first that G is abelian. Let $a,b \in G$. By the Socks-Shoes property, we have $(ab)^{-1} = b^{-1}a^{-1}$, but then $b^{-1}a^{-1} = a^{-1}b^{-1}$ since G is abelian. So $(ab)^{-1} = a^{-1}b^{-1}$.

Now suppose $(ab)^{-1} = a^{-1}b^{-1}$ $\forall a,b \in G$. Let $x,y \in G$. Then by our assumption, $(x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} = xy$, but by the Socks-Shoes property, $(x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$. Thus, $xy = yx$ and G is abelian. ▨

27. For any elements a,b in a group G and any $n \in \mathbb{Z}$, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

Proof The statement holds if $n=0$ since $(a^{-1}ba)^0 = e = a^{-1}ea = a^{-1}b^0a$. Now suppose $n>0$. The statement is certainly true if $n=1$ since $a^{-1}ba = a^{-1}ba$. Proceeding by induction, assume the result holds for n. Then $(a^{-1}ba)^{n+1} = (a^{-1}ba)^n(a^{-1}ba) = (a^{-1}b^n a)(a^{-1}ba)$ $= a^{-1}b^n(aa^{-1})ba = a^{-1}b^n e ba = a^{-1}b^{n+1}a$, so the result holds for $n>0$ by induction.

If $n<0$, then $(a^{-1}ba)^n = ((a^{-1}ba)^{-n})^{-1} \underset{\substack{\uparrow \\ \text{since } -n>0}}{=} (a^{-1}b^{-n}a)^{-1} = a^{-1}b^n a$ by Socks-Shoes (twice). ▨

32. Construct a Cayley table for $U(12)$.

$U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{11}$	$\bar{1}$	$\bar{5}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

33. Suppose the table below is a Cayley table. Fill in the blank entries.

	e	a	b	c	d
e	e	—	—	—	—
a	—	b	—	—	e
b	—	c	d	e	—
c	—	d	—	a	b
d	—	—	—	—	—

The first row + column are easy since $eg = ge = g$ $\forall g \in G$.
We have the relations $a^2 = b$, $ab = c$, $ac = d$, $b^2 = d$, $cb = e$, $c^2 = a$, $da = e$ + $dc = b$.

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Now $cb = e \Rightarrow c = b^{-1}$, $da = e \Rightarrow d = a^{-1}$, so $ad = bc = e$. We also have $d^2 = (a^{-1})^2 = (a^2)^{-1} = b^{-1} = c$. This forces $db = a$ since each column + row contains every element exactly once. Then $cd = b^{-1}a^{-1} = (ab)^{-1} = c^{-1} = b$. This forces $bd = a$, $ba = c$, and $ca = d$.

34. Prove that in a group G, $(ab)^2 = a^2b^2$ iff $ab = ba$.

Proof Let G be a group with $a,b \in G$. If $ab = ba$, then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b$ $= (aa)(bb) = a^2b^2$. Conversely, if $(ab)^2 = a^2b^2$, then $abab = a^2b^2 \Rightarrow a^{-1}abab = a^{-1}a^2b^2 \Rightarrow$ $bab = ab^2 \Rightarrow babb^{-1} = ab^2b^{-1} \Rightarrow ba = ab$. ▨

38. Give an example of a group with elements a, b, c, d, and x s.t. $axb = cxd$ but $ab \neq cd$.

Let $G = D_4$, $a = H$, $b = R_{180}$, $c = D$, $d = R_{270}$, and $x = V$. Then

$$HVR_{180} = R_0 = DVR_{270} \quad \text{but} \quad HR_{180} = V \neq H = DR_{270}. \quad \text{(other examples are possible)}$$

39. Suppose G is a group s.t. $\forall a, b, c, d, x \in G$, $axb = cxd \Rightarrow ab = cd$. Prove that G is abelian.

Proof Let $g, h \in G$. Now $gg^{-1}h = h = hg^{-1}g$, so by the assumed property with $a = g = d$, $x = g^{-1}$, and $b = h = c$, we have $gh = hg$. Thus, G is abelian. ▨

15. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write the following products in the form R^i or $R^i F$, where $0 \leq i < n$:

Using that $FR^kF = R^{-k}$, we have

(a) In D_4: $FR^{-2}FR^5 = (FR^2F)R = R^{-2}R = R^{-1} = \boxed{R^3}$

(b) In D_5: $R^{-3}FR^4FR^{-2} = R^2(FR^4F)R^3 = R^2R^{-4}R^3 = \boxed{R}$

(c) In D_6: $FR^5FR^{-2}F = (FR^5F)R^4F = R^{-5}R^4F = R^{-1}F = \boxed{R^5F}$

17. If G is a group s.t. $x^2 = e$ $\forall x \in G$, then G is abelian.

Proof Let $g, h \in G$. Then $g^2 = e, h^2 = e \Rightarrow g^{-1} = g, h^{-1} = h$. Also, $(gh)^2 = e \Rightarrow (gh)^{-1} = gh$. But by the Socks-Shoes Property, $(gh)^{-1} = h^{-1}g^{-1} = hg$. Thus, $gh = hg$ and G is abelian. ▨

18. Prove that the set S of 3×3 matrices with real entries of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ is a group under matrix multiplication.

Proof Let $A, A' \in S$. Then $AA' = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{bmatrix} \in S$, so the operation is closed. Associativity is inherited from regular matrix multiplication, and the identity matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in S$. According the the above product, we have

$$A^{-1} = \begin{bmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in S.$$ Thus, S is a group. ▨

52. Show that $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \in \mathbb{R}, a \neq 0 \right\}$ is a group under matrix multiplication.

Proof Let $A, B \in G$. Then $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$, so the operation is closed.

Associativity is inherited from regular matrix multiplication.

Since $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, the identity element is $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$.

Finally, the above product implies that $A^{-1} = \begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix} \in G$ ($\frac{1}{a} \in \mathbb{R}$ since $a \neq 0$).

Thus, G is a group. ▨

hrm 6 Let $n > 1$ be a positive integer. Then $(\mathbb{Z}/n\mathbb{Z}, \cdot \bmod n)$ is a binary operation that is associative, has identity $\bar{1}$, and is commutative.

roof In class we showed this was a binary operation. To show associativity, let $a, b, c \in \mathbb{Z}$. Then $\bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot \overline{bc} = \overline{abc} = \overline{ab} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$, so $\cdot$ is associative. If $a \in \mathbb{Z}$, then $\bar{a} \cdot \bar{1} = \bar{a} = \bar{1} \cdot \bar{a}$, so $\bar{1}$ is an identity for $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Finally, let $a, b \in \mathbb{Z}$. Then $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$, so $\cdot$ is commutative. ☒

Chapter 3

1. For each group, find the order of the group + the order of each element in the group.

a) $\mathbb{Z}_{12}$: $|\mathbb{Z}_{12}| = 12$, $|\bar{0}| = 1$, $|\bar{1}| = 12$, $|\bar{2}| = 6$, $|\bar{3}| = 4$, $|\bar{4}| = 3$, $|\bar{5}| = 12$
$|\bar{6}| = 2$, $|\bar{7}| = 12$, $|\bar{8}| = 3$, $|\bar{9}| = 4$, $|\overline{10}| = 6$, $|\overline{11}| = 12$.

b) $U(10) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$: $|U(10)| = 4$, $|\bar{1}| = 1$, $|\bar{3}| = 4$, $|\bar{7}| = 4$, $|\bar{9}| = 2$.

c) $U(12) = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$: $|U(12)| = 4$, $|\bar{1}| = 1$, $|\bar{5}| = 2$, $|\bar{7}| = 2$, $|\overline{11}| = 2$.

d) $U(20) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$: $|U(20)| = 8$, $|\bar{1}| = 1$, $|\bar{3}| = 4$, $|\bar{7}| = 4$, $|\bar{9}| = 2$,
$|\overline{11}| = 2$, $|\overline{13}| = 4$, $|\overline{17}| = 4$, $|\overline{19}| = 2$

e) D_4 : $|D_4| = 8$, $|R_0| = 1$, $|R_{90}| = 4$, $|R_{180}| = 2$, $|R_{270}| = 4$, $|V| = 2$, $|H| = 2$, $|D| = 2$, $|D'| = 2$.

1. Let G be any group and $g \in G$. Then $|g| = |g^{-1}|$.

roof Assume $|g| = n < \infty$. Then $(g^{-1})^n = (g^n)^{-1} = e^{-1} = e$, so $|g^{-1}| \leq n$. Suppose that $(g^{-1})^m = e$ for $m < n$. Then $(g^m)^{-1} = e \Rightarrow g^m = e$, which contradicts $|g| = n$. Thus, $|g^{-1}| = n$. Assume now that $|g| = \infty$. If $(g^{-1})^n = e$ for some $n < \infty$, then $(g^n)^{-1} = e \Rightarrow g^n = e$ - a contradiction. Thus, $|g^{-1}| = \infty$. ☒

9. If $a \in G$ and $|a| = \infty$, prove that $a^m \neq a^n$ when $m \neq n$.

roof Let $m, n \in \mathbb{Z}$ with $m \neq n$. WLOG take $m > n$. Suppose BWOC that $a^m = a^n$. Multiplying on the right by $(a^n)^{-1}$ gives $a^m a^{-n} = a^n a^{-n} \Rightarrow a^{m-n} = e$. This implies $|a| \leq m-n$, which contradicts $|a| = \infty$. Thus, $a^m \neq a^n$. ☒

6. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

roof Let G be a group + let $a, b \in G$ s.t. $|a| = |b| = 2$ and $ab = ba$. We claim that $H = \{e, a, b, ab\}$ is a subgroup of order 4. Clearly, $e \in H$. To check closure under products, we have $a(ab) = a^2 b = b$, $(ab)a = ba^2 = b$, $b(ab) = b^2 a = a$, $(ab)b = ab^2 = a$, and $(ab)(ab) = ab^2 a = a^2 = e$, which are all elements of H (other products are trivial to check). H is also closed under inverses since $a^2 = b^2 = e \Rightarrow a = a^{-1}$, $b = b^{-1}$ and $(ab)^2 = e \Rightarrow ab = (ab)^{-1}$. Thus, H is a subgroup of G. To verify it has order 4, $ab \neq e$ since otherwise $b = a^{-1} = a$, $ab \neq a$ since otherwise $b = e$, and $ab \neq b$ since otherwise $a = e$; all contradictions. Thus, $|H| = 4$ + H is the desired subgroup. ☒

32. If $H, K \leq G$, show that $H \cap K \leq G$.

Proof We have $H \cap K \subseteq G$. Since H is a subgroup, $e_G \in H$; similarly, $e_G \in K$. Thus, $e_G \in H \cap K$. Suppose $a, b \in H \cap K$. Then $ab \in H$ since $a, b \in H$ and H is a subgroup; similarly, $ab \in K$. Thus, $ab \in H \cap K$. Finally, suppose $a \in H \cap K$. Then $a^{-1} \in H$ since $a \in H$ and H is a subgroup; similarly, $a^{-1} \in K$. Thus, $a^{-1} \in H \cap K$, and therefore $H \cap K \leq G$. ▨

37. Suppose G is defined by the given Cayley table

(a) Find the centralizer of each element of G:
$$C_G(1) = G = C_G(5)$$
$$C_G(2) = \{1, 2, 5, 6\} = C_G(6)$$
$$C_G(3) = \{1, 3, 5, 7\} = C_G(7)$$
$$C_G(4) = \{1, 4, 5, 8\} = C_G(8)$$

(b) $Z(G) = \{1, 5\}$

(c) $|1| = 1$, $|2| = 2$, $|3| = 4$, $|4| = 2$, $|5| = 2$, $|6| = 2$, $|7| = 4$, $|8| = 2$. They all divide the order of the group.

41. Prove that $\forall a \in G$, $C_G(a) \leq G$.

Proof We have $C_G(a) \subseteq G$ by definition. Since $ea = ae = a$, we have $e \in C_G(a)$. Suppose that $x, y \in C_G(a)$; then $xa = ax$ and $ya = ay$. We have
$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy), \text{ so } xy \in C_G(a).$$
Finally, suppose $x \in C_G(a)$. Then $xa = ax \Rightarrow xax^{-1} = a \Rightarrow ax^{-1} = x^{-1}a$, so $x^{-1} \in C_G(a)$. Thus, $C_G(a) \leq G$. ▨

42. Prove that $C(H) = \{x \in G \mid xh = hx \ \forall h \in H\}$ is a subgroup of G, where $H \leq G$.

Proof By definition, $C(H) \subseteq G$. Since $eh = he = h$ $\forall h \in H$, we have that $e \in C(H)$. Suppose that $a, b \in C(H)$. Then $(ab)h = a(bh) = a(hb) = (ah)b = (ha)b = h(ab)$ $\forall h \in H$, so $ab \in C(H)$. Finally, let $a \in C(H)$. Then $ah = ha \Rightarrow h = a^{-1}ha \Rightarrow ha^{-1} = a^{-1}h$ $\forall h \in H$, so $a^{-1} \in C(H)$. Thus, $C(H) \leq G$. ▨

43. Must the centralizer of an element of a group be abelian?

No: $C_{D_4}(R_{180}) = D_4$ but D_4 is nonabelian.

44. Must the center of a group be abelian?

Yes: let G be a group and $x, y \in Z(G)$. Then $xy = yx$ since $y \in G$ and $x \in Z(G)$. Thus $Z(G)$ is abelian.

45. Let G be an abelian group with identity e and let $n \in \mathbb{Z}$ be fixed. Prove that $H = \{x \in G \mid x^n = e\}$ is a subgroup of G.

Proof Clearly $H \subseteq G$. Since $e^n = e$, $e \in H$. Let $a, b \in H$. Since G is abelian, we have $(ab)^n = a^n b^n = ee = e$, so $ab \in H$. Let $a \in H$; then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$, so $a^{-1} \in H$. Thus, $H \leq G$. ▨

Give an example of a group G in which $\{x \in G \mid x^2 = e\}$ does not form a subgroup of G.

In $G = D_4$, this set is $\{R_0, R_{180}, V, H, D, D'\}$, which is not a subgroup of D_4.

49. Suppose a group contains elements a, b s.t. $|a| = 4$, $|b| = 2$, and $a^3 b = ba$. Find $|ab|$.

We have $(ab)^2 = a(ba)b = a(a^3 b)b = a^4 b^2 = ee = e$, so $|ab| = 1$ or 2. If $|ab| = 1$, then $ab = e \Rightarrow a^3 b = a^2(ab) = a^2 e = a^2 = ba \Rightarrow a = b$, a contradiction since $|a| \neq |b|$. Thus, we must have $|ab| = 2$.

51. Let $a \in G$ s.t. $|a| = n$ and suppose $d > 0$, $d \mid n$. Prove that $|a^d| = \frac{n}{d}$.

Proof First, we have $(a^d)^{n/d} = a^n = e$, so $|a^d| \leq \frac{n}{d}$. If $|a^d| = m < \frac{n}{d}$, then

$(a^d)^m = a^{dm} = e$, but $dm < n$ contradicts $|a| = n$. Thus, $|a^d| = \frac{n}{d}$. ▨

3. Let $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$ and $H = \{x \in \mathbb{R}^* \mid x^2 \in \mathbb{Q}\}$. Prove that $H \leq \mathbb{R}^*$.

Proof Clearly $H \subseteq \mathbb{R}^*$. Since $1^2 = 1 \in \mathbb{Q}$, $1 \in H$. Let $a, b \in H$. Then $(ab)^2 = a^2 b^2 \in \mathbb{Q}$ since $a^2 \in \mathbb{Q}$, $b^2 \in \mathbb{Q}$, hence $ab \in H$. Let $a \in H$. Then $(a^{-1})^2 = (a^2)^{-1} \in \mathbb{Q}$ since $a^2 \in \mathbb{Q}$ and $a \neq 0$. Thus, $a^{-1} \in H$ and $H \leq \mathbb{R}^*$. ▨

Yes, the exponent 2 can be replaced by any positive integer and still have H be a subgroup.

7. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \ a,b,c,d \in \mathbb{Z} \right\}$ under addition and $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \ \middle| \ a+b+c+d = 0 \right\}$.

Prove that $H \leq G$.

Proof Clearly $H \subseteq G$. The identity element $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H$. Suppose $A, A' \in H$ with

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $A' = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$. Then $A + A' = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix} \in H$ since

$a+a' + b+b' + c+c' + d+d' = (a+b+c+d) + (a'+b'+c'+d') = 0 + 0 = 0$. If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H$,

then $A^{-1} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in H$ since $-a-b-c-d = -(a+b+c+d) = -0 = 0$. Hence, $H \leq G$. ▨

We cannot replace 0 by 1, since $(a+b+c+d) + (a'+b'+c'+d') = 1+1 = 2 \neq 1 \Rightarrow H$ is not closed under addition.

10. Let $G = \{ f : \mathbb{R} \to \mathbb{R}^* \mid f \text{ a function} \}$ under multiplication of functions. Let $H = \{ f \in G \mid f(2) = 1 \}$.

Prove that $H \leq G$.

Proof Clearly $H \subseteq G$. The identity in G is $e(x) \equiv 1$, and since $e(2) = 1$, we have $e \in H$.

Suppose $f, g \in H$. Then $(fg)(2) = f(2)g(2) = 1 \cdot 1 = 1 \Rightarrow fg \in H$. If $f \in H$, then

$f^{-1}(2) = \frac{1}{f(2)} = \frac{1}{1} = 1 \Rightarrow f^{-1} \in H$. Thus, $H \leq G$. ▨

Yes, 2 can be replaced by any real number.

3. Let $H = \{a+bi \mid a,b \in \mathbb{R}, a^2+b^2=1\}$. Prove or disprove that $H \leq (\mathbb{C}^*, \cdot)$. Describe the elements of H geometrically.

Proof Certainly $H \subseteq \mathbb{C}^*$ since $0 \notin H$. The identity element $1+0i \in H$ since $1^2+0^2=1$.
Suppose $a+bi, c+di \in H$. Then $(a+bi)(c+di) = (ac-bd)+(bc+ad)i$ and
$(ac-bd)^2+(bc+ad)^2 = a^2c^2 - 2abcd + b^2d^2 + b^2c^2 + 2abcd + a^2d^2 = a^2c^2+b^2d^2+b^2c^2+a^2d^2$
$= a^2(c^2+d^2)+b^2(c^2+d^2) = (a^2+b^2)(c^2+d^2) = 1 \cdot 1 = 1$. Thus, $(a+bi)(c+di) \in H$.
Let $a+bi \in H$. Then $(a+bi)^{-1} = a-bi$ since $(a+bi)(a-bi) = a^2+b^2 = 1$. Also, $a-bi \in H$ since $a^2+(-b)^2 = a^2+b^2 = 1$. Thus, $H \leq \mathbb{C}^*$. ▨

H is the set of points on the unit circle in the complex plane.

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

Proof By assumption, $\exists\, x \in G$ s.t. $x \neq e$. Let $|x| = n$. Since $x \neq e$, $n > 1$. If n is prime, then we are done, so assume n is composite. Then there is a prime p and an integer m s.t. $n = pm$ by the FTA. Then $x^m \in G$ and by #51 we have $|a^m| = \frac{n}{m} = p$. ▨