Debra Griffin
Math 210A
HW #2, 2.3 p. 61 #18, 21 – 28

2.18 Assume that G is a set with an associative binary operation. Prove that $(ab)(cd) = a[(bc)d]$ without using generalized associativity.

Proof:
If G is a set with an associative binary operation and $a, b, c, d \in G$, then $(ab)(cd) = a[b(cd)] = a[(bc)d]$, as desired.

2.21 If G is a group, prove that the only element $g \in G$ with $g^2 = g$ is 1.

Proof:
Assume $g \in G$ with $g^2 = g$. Then $g^{-1} \in$ G and multiplying both sides by g^{-1} gives us $g = g^2 * g^{-1} = g * g^{-1} = e$.

2.22 This exercise gives a shorter list of axioms defining a group. Let H be a set containing an element e, and assume that there is an associative binary operation $*$ on H satisfying the following properties:
1. $e * x = x$ for all $x \in H$;
2. for every $x \in H$, there is $x' \in H$ with $x' * x = e$.

(i) Prove that if $h \in H$ satisfies $h * h = h$, then $h = e$.

Hint: If $h' * h = e$, evaluate $h' * h * h$ in two ways.

Proof:

If $h \in H$ satisfies $h * h = h$, then $h = e * h = h' * h * h = h' * h = e$. $\therefore$ $h = e$.

(ii) For all $x \in H$, prove that $x * x' = e$.

Hint: Consider $(x * x')^2$.

Proof:

For all $x \in H$, $(x * x')^2 = (x * x')(x * x') = x * (x' * x) * x' = x * e * x' = x * x'$.

By result in (i), $(x * x')^2 = x * x' \Rightarrow x * x' = e$.

(iii) For all $x \in H$ prove that $x * e = x$.

Hint: Evaluate $x * x' * x$ in two ways.

Proof: Since $*$ is associative, then $x * e = x * (x' * x) = (x * x') * x = e * x = x$.

(iv) Prove that if $e' \in H$ satisfies $e' * x = x$ for all $x \in H$, then $e' = e$.

Hint: Show that $(e')^2 = e'$.

Proof:
If $e' \in H$ satisfies $e' * x = x$ for all $x \in H$, then $(e')^2 = e' * e' = e'$.

Again by (i), $e' = e$.

(v) Let $x \in H$. Prove that if $x'' \in H$ satisfies $x'' * x = e$, then $x'' = x'$.

Hint: Evaluate $x' * x * x''$ in two ways.

Proof:
If $x'' \in H$ satisfies $x'' * x = e$, then by (ii), $x * x'' = e$.

$\therefore\ x' = x' * e = x' * x * x'' = e * x'' = x''$.

(vi) Prove H is a group.

Proof:

By (i), if $h \in H$ satisfies $h * h = h$, then $h = e$.

This gives us cancellation for $h * h = h$.

By (ii), for all $x \in H$, $x * x' = e$.

This gives us an element x' such that $x' * x = e = x * x'$.

By (iii), for all $x \in H$, $x * e = x$.

This gives us that H has an element, e, such that $\forall\ x \in \mathrm{H}$, $e * x = x = x * e$.

By (iv), if $e' \in H$ satisfies $e' * x = x$ for all $x \in H$, then $e' = e$.

This give us uniqueness of the identity, e.

By (v), if $x'' \in H$ satisfies $x'' * x = e$, then $x'' = x'$.

This gives us uniqueness of each inverse.

$\therefore$ We have a set H equipped with a binary operation $*$ such that

(i) the associative law holds;

(ii) there is an element $e \in H$, with $e * x = x = x * e$ for all $x \in H$;

(iii) every $x \in H$ has an inverse; there is $x' \in H$ with $x * x' = e = x' * x$.

$\therefore$ H is a group.

2.23 Let y be a group element of order m; if $m = pt$ for some prime p, prove that y^t has order p. **Hint**: Clearly, $(y^t)^p = 1$. Use Theorem 2.24 to show that no smaller power of y^t is equal to 1.

Proof:

Assume $\circ(y) = m = pt$ for some prime p, then $1 = y^m = y^{pt} = (y^t)^p$.

Suppose $\exists\ d < p$ such that $(y^t)^d = 1$. Then $td \mid m$ by Theorem 2.24 (*If $a \in$ G is an element of order n, then $a^m = 1$ if and only if $n \mid m$.*) However, $d \nmid p$ as p is prime, hence $td \nmid pt = m$.

$\therefore\ \circ(y^t) = p$.

2.24 Let G be a group and let $a \in G$ have order k. If p is a prime divisor of k, and if there is $x \in$ G with $x^p = a$, prove that x has order pk.

Proof (My newer elegant proof): ☺

Since $\circ(a) = k$ and $x^p = a$, then $x^{pk} = (x^p)^k = a^k = 1$.

$\therefore\ x$ has finite order, w, such that $w \mid pk$. This gives us that $k \mid w$.

Since p is a prime divisor of k, then $p \mid k \mid w$. So then we have that w/p is an integer.

Now, $\left(x^p\right)^{\frac{w}{p}} = x^w = 1$, hence $k \mid (w/p)$ or $kp \mid w$.

$\therefore\ w = pk$, the order of x.

Earlier Proof:

Since $\circ(a) = k$ and $x^p = a$, then $x^{pk} = (x^p)^k = a^k = 1$.

$\therefore\ x$ has finite order, w, such that $w \mid pk$, hence $pk = wm$.

So, $a^w = (x^p)^w = (x^w)^p = 1^p = 1$. This gives us that $k \mid w$, hence $w = km'$.

So $pk = wm = km'm$, hence $p = m'm$.

Since p is prime, then $m' = 1$ and $m = p$ or $m' = p$ and $m = 1$.

Suppose $m' = 1$ and $m = p$, then $pk = wp$, hence $k = w$.

Since p is a prime divisor of k, then for some $t \in \mathbb{Z}^+$ such that $t < k$, $k = pt$.

So $1 = x^w = x^k = x^{pt} = a^t$, a contradiction (as $\circ(a) = k$).

$\therefore\ m' = p$ and $m = 1$, which gives us $pk = w \bullet 1 = w$. $\therefore\ \circ(x) = pk$.

2.25 Let G = GL(2, Q), and let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$.

Show that $A^4 = I = B^6$, but that $(AB)^n \neq I$ for all $n > 0$, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the 2 × 2 identity matrix. Conclude that AB can have infinite order even though both factors A and B have finite order (this cannot happen in a finite group).

Proof:

$$A^4 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$B^6 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \qquad (AB)^2 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \bullet \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

Clearly, $\forall\ n > 1$, $(AB)^n = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $\therefore$ AB has infinite order.

2.26 If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be Abelian. [The Boolean groups $B(X)$ of Example 2.18 are such groups.]

Proof:

Let $a, b \in G$. Then $ab \in G$.

We are given that $x^2 = 1$ for every $x \in G$, and so $1 = (ab)^2 = a^2 \bullet b^2$. Thus, $abab = aabb$.

Left multiplying by a^{-1} and right multiplying by b^{-1} gives us $ba = ab$.

$\therefore$ G is Abelian.

2.27 If G is a group with an even number of elements, prove that the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.

Hint: Pair each element with its inverse.

Proof:

Let $S = \{a \in \mathrm{G}: \circ(a) \geq 3\}$. Then $\forall\ a \in \mathrm{S}, \exists\ a^{-1} \in \mathrm{S}$ such that $a \neq a^{-1}$.

This gives us a pairing of each element in S with its inverse, hence $|S|$ is even.

Let $M = \{b \in G: \circ(b) < 3\}$. Then $|M| = |G| - |S|$, hence $|M|$ is even.

Since 1 has order 1, then $1 \in M$ and all other elements in M have order 2.

$\therefore$ The number of elements of order 2 in G is odd.

In fact, since $1 \in G$ and $|M|$ is even, there must be at least one element of order 2.

2.28 What is the largest order of an element in S_n, where $n = 1, 2, \ldots, 10$? (We remark that no general formula is known for arbitrary n, although, in 1903, E. Landau found the asymptotic behavior.)

Proof:

n	S_n Cycle structures/Orders	Largest order element
1	$\circ(1) = 1$	1
2	$\circ(1) = 1$, $\circ(12) = 2$	2
3	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$	3
4	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$, $\circ(1234) = 4$, $\circ(12)(34) = 2$	4
5	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$, $\circ(1234) = 4$, $\circ(12345) = 5$, $\circ(123)(45) = 6$	6
6	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$, $\circ(1234) = 4$, $\circ(12345) = 5$, $\circ(123456) = 6$, $\circ(12)(45)(56) = 2$, $\circ(12)(3456) = 4$, $\circ(123)(456) = 3$	6
7	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$, $\circ(1234) = 4$, $\circ(12345) = 5$, $\circ(123456) = 6$, $\circ(1234567) = 7$, $\circ(12)(45)(56) = 2$, $\circ(12)(34567) = 10$, $\circ(123)(4567) = 12$	12
8	$\circ(1) = 1$, $\circ(12) = 2$, $\circ(123) = 3$, $\circ(1234) = 4$, $\circ(12345) = 5$, $\circ(123456) = 6$, $\circ(1234567) = 7$, $\circ(12345678) = 8$, $\circ(12)(45)(56)(78) = 2$, $\circ(123)(45678) = 15$, $\circ(1234)(5678) = 4$	15

9	∘(1) = 1, ∘(12) = 2, ∘(123) = 3, ∘(1234) = 4, ∘(12345) = 5, ∘(123456) = 6, ∘(1234567) = 7, ∘(12345678) = 8, ∘(123456789) = 9, ∘(12)(45)(56)(78) = 2, ∘(12)(34)(56)(789) = 6, ∘(123)(456)(789) = 3, ∘(123)(456789) = 6, ∘(1234)(5678) = 4, ∘(1234)(56789) = 20	20
10	∘(1) = 1, ∘(12) = 2, ∘(123) = 3, ∘(1234) = 4, ∘(12345) = 5, ∘(123456) = 6, ∘(1234567) = 7, ∘(12345678) = 8, ∘(123456789) = 9, ∘(123456789 10) = 10, ∘(12)(45)(56)(78)(9 10) = 2, ∘(12)(34)(56)(789 10) = 4, ∘(12)(34)(567)(89 10) = 6, ∘(12)(345)(6789 10) = 30, ∘(123)(456)(789) = 3, ∘(123)(456789 10) = 21, ∘(1234)(56789) = 20, ∘(1234)(56789 10) = 12, ∘(12345)(12345) = 25,	30