HW 2 Solutions M31F11

3.7| In the Cayley table for a finite group G, each element occurs precisely once in each row and once in each column.

Proof| Suppose that some element x occurs twice in a row of the Cayley table. In other words, $x = ab = ac$ for some $a, b, c \in G$, with $b \neq c$. But by Theorem 3.6 (i), $ab = ac$ implies $b = c$, a contradiction. Therefore, every element that appears in a row of the Cayley table must be distinct; that is, at most $|G|$ elements can appear in each row. But since each row of the Cayley table contains as many elements as there are elements in G, it follows that every element of G must appear in each row of the Cayley table. Thus, every element of G appears precisely once in each row. ☒

The proof for the other assertion is almost identical; appeal to Theorem 3.6 (ii) to see uniqueness, and replace "row" by "column" and vice versa in the argument that every element must appear at least once. (But I xpect students to write out this proof in full detail!)

3.12 A group G is abelian iff $x^2y^2 = (xy)^2$ for all $x, y \in G$.

Proof If G is abelian, then
$$(xy)^2 = xyxy = xxyy = x^2y^2,$$
by commutativity.

Now, suppose $(xy)^2 = x^2y^2$ ☺ for all $x, y \in G$. We need to show G is abelian; that is, we need to show that $ab = ba$ (*) for all $a, b \in G$. Observe that this is the same as asserting that $aba^{-1} = b$ for all $a, b \in G$ (multiply (*) on the right by a^{-1}).

Consider the equation ☺. Multiplying both sides on the right by $(xy)^{-1} = y^{-1}x^{-1}$ results in the equation
$$xy = x^2y^2y^{-1}x^{-1} = x^2yx^{-1}$$

Applying Theorem 3.6 (i), this tells us that $y = xyx^{-1}$, and hence that $yx = xy$ for all x, y in G. Therefore, G is commutative. ☒

HW2 Solutions M31 F11

If $(G, *)$ is a group with identity e, and f is a left identity for G, then $e = f$.

<u>Proof</u> Since e is an identity, $e * x = x * e = x$ for all x in G. Since f is a left identity, $f * x = x$ for all x in G. But then, by Theorem 3.6 (ii) [cancellation laws] we have

$$e * x = f * x \Rightarrow e = f.$$

HW 2 Solutions M31F11

4.15 (a) Find $(123, 321)$ and find $x, y \in \mathbb{Z}$ such tha
$123x + 321y = (123, 321)$.

$$321 = 2\cdot 123 + (321-246) = 2\cdot 123 + 75$$
$$123 = 1\cdot 75 + (123-75) = 1\cdot 75 + 48$$
$$75 = 1\cdot 48 + (75-48) = 1\cdot 48 + 27$$
$$48 = 1\cdot 27 + (48-27) = 1\cdot 27 + 21$$
$$27 = 1\cdot 21 + (27-21) = 1\cdot 21 + 6$$
$$21 = 3\cdot 6 + (21-18) = 3\cdot 6 + 3$$
$$6 = 2\cdot 3 + 0$$

Thus $\boxed{(123, 321) = 3.}$

We work backwards to find x & y:

$$\begin{aligned}
3 &= 1\cdot 21 - 3\cdot 6 \\
&= 1\cdot 21 - 3\cdot(27-21) = 4\cdot 21 - 3\cdot 27 \\
&= 4(48-27) - 3\cdot 27 = 4\cdot 48 - 7\cdot 27 \\
&= 4\cdot 48 - 7(75-48) = 11\cdot 48 - 7\cdot 75 \\
&= 11\cdot(123-75) - 7\cdot 75 = 11\cdot 123 - 18\cdot 75 \\
&= 11\cdot 123 - 18(321 - 2\cdot 123) = 47\cdot 123 - 18\cdot 321
\end{aligned}$$

So $\boxed{x = 47,\ y = -18}$

HW2 M31 F11 Solutions

4.21 Show that for any two elements x, y of any group G, $o(xy) = o(yx)$.

Proof Suppose first that $o(xy) = n < \infty$ is finite. In other words, $\underbrace{xy\,xy \cdots xy}_{n \text{ times}} = e$ ☺ and

$\underbrace{xyxy \cdots xy}_{m} \neq e$ for all $m < n$.

Multiply the equation ☺ by x^{-1} on the left, and by y^{-1} on the right, so that ☺ becomes

$$\underbrace{yx\,yx \cdots yx}_{n-1} = x^{-1}y^{-1} = (yx)^{-1}$$

Thus, $\underbrace{yxyx \cdots yx}_{n} = e$. In other words, $o(yx) \leq n$.

Suppose $o(yx) = m < n$. In other words, $\overbrace{yx\,yx \cdots yx}^{m} = e$. If we multiply this equation by y^{-1} on the left and by x^{-1} on the right, we see that $\overbrace{xy\,xy \cdots xy}^{m-1} = y^{-1}x^{-1} = (xy)^{-1}$,

so $(xy)^m = e$ and $o(xy) \leq m < n$, which is a contradiction.

Therefore, $o(xy) = o(yx) = n$.

If $o(xy) = \infty$, suppose (for a contradiction) that $o(yx) = n < \infty$. Then, as we showed above, $o(xy) \leq n$ because $(xy)^n = e$, and this contradicts our hypothesis that $o(xy) = \infty$. Therefore, $o(yx) = \infty$ also. ☒

HW 2 Solutions M31 F11

4.23 If x, y are elements of an abelian group G, and $(o(x), o(y)) = 1$, then $o(xy) = o(x)o(y)$.

Proof. Let $o(x) = m$, $o(y) = n$. By 4.22, we know that $o(xy) \mid mn$. We need to show that $k := o(xy)$ can't be less than $o(x)o(y) = mn$.

Writing $k = o(xy)$, we see that

$$(xy)^k = x^k y^k = e.$$

Therefore, $x^k = (y^k)^{-1}$. By Theorem 4.4 (i), that implies that $o(x^k) = o((y^k)^{-1}) = o(y^k)$.

By Theorem 4.4 (iii), $o(x^k) = n/(n,k)$ and $o(y^k) = m/(m,k)$.

In other words, $\dfrac{n}{(n,k)} = \dfrac{m}{(m,k)}$.

Since $n/(n,k)$ divides n, and $(n,m) = 1$, we must also have $(m, n/(n,k)) = 1$ [otherwise, if $(m, n/(n,k)) = d > 1$, then d divides m and also $n/(n,k)$, and so $d \mid n$ as well]. Therefore, by Theorem 4.3, since $m \mid (m,k) \cdot \dfrac{n}{(n,k)}$, we must have $m \mid (m,k)$.

Therefore, k must be a multiple of m.

The same argument applied to n shows that

[over]

4.23 cont.'d

Since $\frac{n}{(n,k)} = \frac{m}{(m,k)}$, we have $n \mid \frac{m}{(m,k)} \cdot (n,k)$,

and since $(n,m)=1$, we must have $n \mid (n,k)$, and so n divides k.

Thus, $k \geq \text{lcm}(n,m) = nm$ since $(n,m)=1$.

But by Problem 4.22, we know $k \leq mn$, and so we must have $k = mn$.

In other words, $o(xy) = o(x)\,o(y)$ as claimed. $\boxtimes$

HW 2 Solutions M31 F11

4.3 Let $X = \{1,2,3,4,5\}$ and let $A = \{1,4,5\}$. There are 2 elements in $\langle A \rangle$ in $(P(X), \Delta)$.

Proof By definition, $\langle A \rangle = \{A, A^2, A^3, \ldots\}$

$$= \{A, A \Delta A, A \Delta A \Delta A, \ldots\}$$

By Theorem 4.5, $= \{A, \emptyset\}$

(We know we can stop taking powers after we reach $\emptyset$, because $\emptyset$ is the identity in $(P(X), \Delta)$.)

HW2 Solutions M31F11

4.22 Let G be an abelian group and $x, y \in G$ elements of finite order. Then xy is also of finite order, and in fact $o(xy) \mid o(x)o(y)$.

Proof. Suppose $o(x)=n$ and $o(y)=m$. Then,

$$(xy)^{mn} = x^{mn}y^{mn}$$

because G is abelian, and $x^{mn}y^{mn} = (x^n)^m(y^m)^n = e^m e^n = e$.

Therefore $\overset{mn=}{o(x)o(y)}$ is a multiple of $o(xy)$, by Theorem 4.4 (ii).

$\boxtimes$

4.25 If $|G|$ is even, then there is an element $x \in G$ with $x^2 = e$, but $x \neq e$.

Proof: Suppose that for every $x \neq e$ in G, $x^2 \neq e$. Then we can form a bunch of 2-element subsets of G: $\{x, x^2\}$; $\{y, y^2\}$ for any $y \notin \{x, x^2\}$; $\{z, z^2\}$ for any $z \notin \{x, x^2\} \cup \{y, y^2\}$; etc. [Note that $x \neq x^2$ for every $x \neq e$.]

We can continue this process as long as there is a non-identity element in G that we haven't chosen yet. Thus, every element but e will end up in some 2-element subset.

However, the total number of elements in the 2-element subsets is even, so

$$|G| = \underset{\text{for } e}{1} + 2\underset{\text{number of 2-element subsets}}{K}$$

which is not even – contradiction.

Therefore, we must have at least one element $x \in G$ such that $x^2 = e$, as claimed. ☒

HW 2 Solutions M31 F11

The set $\{1, 6, 11, 16, 26, 31\}$ forms a (cyclic) group under multiplication mod 35.

Proof We know the operation is associative, since multiplication is associative on $\mathbb{Z}$. The set has a multiplicative identity: 1.

The group is generated by the elements 31 and 26: for example,

$$31^0 = 1$$
$$31^1 = 31$$
$$31^2 = 961 \equiv 16 \pmod{35}$$
$$31^3 \equiv 16 \cdot 31 = 49 \equiv 6 \pmod{35}$$
$$31^4 \equiv 31 \cdot 6 = 186 \equiv 11 \pmod{35}$$
$$31^5 \equiv 31 \cdot 11 = 341 \equiv 26 \pmod{35}$$
$$31^6 \equiv 31 \cdot 26 = 806 \equiv 1 \pmod{35}$$

This also shows us that every element of the group has an inverse: If $x \in \{1, 6, 11, 16, 26, 31\}$, write $x = 31^n$. Then $x^{-1} = 31^{6-n}$ is also an element of the group, and $31^n \cdot 31^{6-n} = 31^6 \equiv 1 \pmod{35}$. ⊠