Math 620: §3.4 Isomorphisms and §3.5 Cyclic Groups

Due on Monday, October 26, 2015

Boynton 10:00

Kailee Gray

Exercise 3.4.10

Show that the group $\{f_{m,b} : \mathbb{R} \to \mathbb{R} \mid f(x) = mx + b, m \neq 0\}$ of affline functions from $\mathbb{R}$ to $\mathbb{R}$ (under composition of functions) is isomorphic to the group of all 2×2 matrices over $\mathbb{R}$ of the form $M = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$ (under matrix multiplication).

Proof. Let $A = \{f_{m,b} : \mathbb{R} \to \mathbb{R} \mid f(x) = mx + b, m \neq 0\}$ and let

$F = \left\{ B \in M(2, \mathbb{R}) | \ B \text{ is of the form } \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \right\}$. Define $\varphi : A \to F$ by $\varphi\left(f_{m,b}\right) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$.

(one-to-one) Consider $f_{a,b},\ f_{c,d} \in A$ where $\varphi(f_{a,b}) = \varphi(f_{c,d})$. Then, $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$ so $a = c$ and $b = d$. Therefore, $ax = cx$, so $ax + b = cx + d$. Thus, $f_{a,b} = f_{c,d}$.

(onto) Let $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in F$. Then, $f(x) = mx + b \in A$ and $\varphi(f(x)) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$.

(homomorphism) Let $f_{a,b},\ f_{c,d} \in A$ so $a, b, c, d \in \mathbb{R}$ and $a, c \neq 0$. Then, $f_{a,b} \circ f_{c,d} = a(cx + d) + b = acx + ad + b$.

So $\varphi(f_{a,b} \circ f_{c,d}) = \varphi(f(x) = acx + ad + b) = \begin{bmatrix} ac & ad + b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \varphi(f_{a,b})\varphi(f_{c,d})$

Thus, φ is a group isomorphism from A to F which, by definition 3.4.1, implies $A \cong F$. $\square$

Exercise 3.4.13: Let C_2 be the subgroup $\{\pm 1\}$ of the multiplicative group $\mathbb{R}^\times$. Show that $\mathbb{R}^\times$ is isomorphic to $\mathbb{R}^+ \times C_2$.

Define $\varphi : \mathbb{R}^\times \to \mathbb{R}^+ \times C_2$ by $\varphi(r) = (|r|, \frac{r}{|r|})$. Notice $|r| = r$ if $r > 0$ and $|r| = -r$ if $r < 0$, so $\frac{r}{|r|} = \pm 1 \in C_2$. Also, $|r| > 0$ implies $|r| \in \mathbb{R}^+$ Since $r \in \mathbb{R}^\times$ implies $r \neq 0$, φ is well defined.

(one-to-one) Consider $r_1, r_2 \in \mathbb{R}^\times$ where $\varphi(r_1) = \varphi(r_2)$. Then, $(|r_1|, \frac{r_1}{|r_1|}) = (|r_2|, \frac{r_2}{|r_2|})$ so $|r_1| = |r_2|$ and $\frac{r_1}{|r_1|} = \frac{r_2}{|r_2|}$. $|r_1| = |r_2|$ implies $r_1 = \pm r_2$. However, $\frac{r_1}{|r_1|} = \frac{r_2}{|r_2|}$ implies $\frac{r_1}{r_2} = \frac{|r_1|}{|r_2|}$ and so $\frac{r_1}{r_2} > 0$. Thus, either $r_1 > 0$ and $r_2 > 0$ or $r_1 < 0$ and $r_2 < 0$. Suppose $r_1 > 0$ and $r_2 > 0$. Then, $|r_1| = r_1$ and $|r_2| = r_2$ so $r_1 = r_2$. If $r_1 < 0$ and $r_2 < 0$, $|r_1| = -r_1$ and $|r_2| = -r_2$ so $-r_1 = -r_2$ implies $r_1 = r_2$.

(onto) Consider $(r, c) \in \mathbb{R}^+ \times C_2$. Then, $r > 0$ and $c = \pm 1$. First, consider $(r, 1) \in \mathbb{R}^+ \times C_2$. Then, for some $r \in \mathbb{R}^\times$ such that $r > 0$, $\varphi(r) = (|r|, \frac{r}{|r|}) = (r, \frac{r}{r}) = (r, 1) \in \mathbb{R}^+ \times C_2$. Next, consider $(r, -1) \in \mathbb{R}^+ \times C_2$. For some $r \in \mathbb{R}^\times$ such that $r < 0$, $\varphi(r) = (|r|, \frac{r}{|r|}) = (-r, \frac{r}{-r}) = (-r, -1) \in \mathbb{R}^+ \times C_2$.

(homomorphism) Let $r_1, r_2 \in \mathbb{R}^\times$ so $r_1, r_2 \neq 0$. Then, $\varphi(r_1 r_2) =$

$$\left(r_1 r_2, \frac{r_1 r_2}{|r_1 r_2|}\right) = \left(r_1 \cdot r_2, \frac{r_1 r_2}{|r_1||r_2|}\right) = \left(r_1 \cdot r_2, \frac{r_1}{|r_1|} \cdot \frac{r_2}{|r_2|}\right) = \left(r_1, \frac{r_1}{|r_1|}\right) \cdot \left(r_2, \frac{r_2}{|r_2|}\right) = \varphi(r_1)\varphi(r_2).$$

Thus, φ defines a group isomorphism from $\mathbb{R}^\times$ to $\mathbb{R}^+ \times C_2$ which, by definition 3.4.1, implies $\mathbb{R}^\times \cong \mathbb{R}^+ \times C_2$.

Exercise 3.4.15: Let G be any group, and let a be a fixed element of G. Define a function $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$ for all $x \in G$. Show that ϕ_a is an isomorphism.

Proof. Let G be any group, and let a be a fixed element of G. Define a function $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$ for all $x \in G$.
(one-to-one) Consider $x_1, x_2 \in G$ where $\phi(x_1) = \phi(x_2)$. Then, $ax_1a^{-1} = ax_2a^{-1}$. Notice

$$\begin{array}{lll}
ax_1a^{-1}a & = ax_2a^{-1}a & \text{multiply on the right by } a \\
ax_1e & = ax_2e & \text{because } a^{-1}a = e, \text{ the identity element in } G \\
a^{-1}ax_1 & = a^{-1}ax_2 & \text{because } x_1e = x_1 \text{ and } x_2e = x_2. \text{ Then, multiply on the left by } a^{-1} \\
ex_1 & = ex_2 & \text{because } a^{-1}a = e \\
x_1 & = x_2 & \text{because } ex_1 = x_1 \text{ and } ex_2 = x_2
\end{array}$$

(onto) Consider $x_1 \in G$. Then, $a, a^{-1} \in G$ implies $a^{-1}x_1a \in G$, so

$$\begin{aligned}
\phi(a^{-1}x_1a) &= a(a^{-1}x_1a)a^{-1} && \text{by definition of } \phi \\
&= (aa^{-1})x_1(aa^{-1}) && G \text{ is a group so the operation of } G \text{ is associative} \\
&= (e)x_1(e) && \text{because } aa^{-1} = e \\
&= (ex_1)(e) && G \text{ is a group so the operation of } G \text{ is associative} \\
&= x_1 && \text{definition of the identity element}
\end{aligned}$$

(homomorphism) Let $x_1, x_2 \in G$. Then, by the associative law of G and the definition of the identity element and inverses in G we have,

$$\phi(x_1x_2) = a(x_1x_2)a^{-1} = a(x_1ex_2)a^{-1} = a(x_1(a^{-1}a)x_2)a^{-1} = (ax_1a^{-1})(ax_2a^{-1}) = \phi(x_1)\phi(x_2).$$

Thus, ϕ defines a group isomorphism from G to G. □

Exercise 3.4.16: Let G be any group. Define $\phi : G \to G$ by $\phi(x) = x^{-1}$, for all $x \in G$.

(a) Prove that ϕ is one-to-one and onto.

Proof. **(one-to-one)** Consider $x_1, x_2 \in G$ and suppose $\phi(x_1) = \phi(x_2)$. Then, $x_1^{-1} = x_2^{-1}$. Since $x_1^{-1}, x_2^{-1} \in G$, x_1^{-1}, x_2^{-1} have inverses in G, so $(x_1^{-1})^{-1} = (x_2^{-1})^{-1}$. Thus, $x_1 = x_2$.
(onto) Let $x \in G$. Then, $x^{-1} \in G$ and $\phi(x^{-1}) = (x^{-1})^{-1} = x$. $\square$

(b) Prove that ϕ is an isomorphism if and only if G is abelian.

Proof. ($\Rightarrow$) Assume ϕ is an isomorphism. Then, ϕ is a homomorphism, so for any x_1, x_2, $\phi(x_1x_2) = \phi(x_1)\phi(x_2)$. Since $\phi(x_1x_2) = (x_1x_2)^{-1} = x_2^{-1}x_1^{-1}$ and $\phi(x_1)\phi(x_2) = x_1^{-1}x_2^{-1}$. Thus, $x_2^{-1}x_1^{-1} = x_1^{-1}x_2^{-1}$ implies $(x_2^{-1}x_1^{-1})^{-1} = (x_1^{-1}x_2^{-1})^{-1}$. Further, $(x_1^{-1})^{-1}(x_2^{-1})^{-1} = (x_2^{-1})^{-1}(x_1^{-1})^{-1}$. Equivalently, $x_1x_2 = x_2x_1$. Thus, G is abelian.
($\Leftarrow$) Assume G is abelian. Then, for any $x_1, x_2 \in G$, $x_1x_2 = x_2x_1$. We can follow our previous argument backwards to obtain

$$
\begin{aligned}
x_1x_2 &= x_2x_1 \\
(x_1^{-1})^{-1}(x_2^{-1})^{-1} &= (x_2^{-1})^{-1}(x_1^{-1})^{-1} \\
(x_2^{-1}x_1^{-1})^{-1} &= (x_1^{-1}x_2^{-1})^{-1} \\
x_2^{-1}x_1^{-1} &= x_1^{-1}x_2^{-1} \\
(x_1x_2)^{-1} &= \phi(x_1)\phi(x_2) \\
\phi(x_1x_2) &= \phi(x_1)\phi(x_2)
\end{aligned}
$$

Thus, ϕ is a homomorphism. From part (a), we know ϕ is one-to-one and onto. Thus, ϕ is an isomorphism. $\square$

Exercise 3.4.22: Let a, b be positive integers, and let gcd$(a, b) = d$ and $m =$ lcm$[a, b]$. Write $d = sa + tb$, $a = a'd$, and $b = b'd$. Prove that the function $f : \mathbb{Z}_m \times \mathbb{Z}_d \to \mathbb{Z}_a \times \mathbb{Z}_b$ defined by $f(([x]_m, [y]_d)) = ([x + ysa']_a, [x - ytb'])_b$ is an isomorphism.

Proof. **(well-defined)** Suppose there exists elements in $\mathbb{Z}_m \times \mathbb{Z}_d$ such that $([x_1]_m, [y_1]_d) = ([x_2]_m, [y_2]_d)$. Then,

$$x_1 \equiv x_2 \pmod{m} \text{ and } y_1 \equiv y_2 \pmod{d}. \tag{1}$$

$$\text{Equivalently, for some } l, k \in \mathbb{Z}, \quad x_1 = x_2 + lm \text{ and } y_1 = y_2 + kd \tag{2}$$

Since $a|m$, we can write (2) as $x_1 = x_2 + ll'a$ for some $l' \in \mathbb{Z}$. Thus, $x_1 \equiv x_2 \pmod{a}$. Also from (2), we can multiply by a' to obtain $a'y_1 = a'y_2 + a'kd$ which, because $a'd = a$, we can write $a'y_1 = a'y_2 + ka$. Multiplying by s, we have $sa'y_1 = sa'y_2 + ska$; equivalently $sa'y_1 \equiv sa'y_2 \pmod{a}$. Thus, since $x_1 \equiv x_2 \pmod{a}$ and $sa'y_1 \equiv sa'y_2 \pmod{a}$, we have

$$x_1 + sa'y_1 \equiv x_2 + sa'y_2 \pmod{a} \tag{3}$$

Similarly, since $b|m$, we can write (2) as $x_1 = x_2 + ll''b$ for some $l'' \in \mathbb{Z}$. Thus, $x_1 \equiv x_2 \pmod{b}$. Also from (2), we can multiply by b' to obtain $b'y_1 = b'y_2 + b'kd$ which, because $b'd = b$, we can write $b'y_1 = b'y_2 + kb$. Multiplying by $-t$, we have $-tb'y_1 = -tb'y_2 - tkb$; equivalently $-tb'y_1 \equiv -tb'y_2 \pmod{b}$. Thus, since $x_1 \equiv x_2 \pmod{b}$ and $-tb'y_1 \equiv -tb'y_2 \pmod{b}$, we have

$$x_1 - tb'y_1 \equiv x_2 - tb'y_2 \pmod{b} \tag{4}$$

Equations (3) and (4) imply $f(([x_1]_m, [y_1]_d)) = f(([x_2]_m, [y_2]_d))$.
(homomorphism) Consider any $([x_1]_m, [y_1]_d), ([x_2]_m, [y_2]_d)$ in $\mathbb{Z}_m \times \mathbb{Z}_d$. Then, $([x_1]_m, [y_1]_d) + ([x_2]_m, [y_2]_d) = ([x_1]_m + [x_2]_m, [y_1]_d + [y_2]_d)$. By proposition 1.4.2, $([x_1]_m + [x_2]_m, [y_1]_d + [y_2]_d) = ([x_1 + x_2]_m, [y_1 + y_2]_d)$. Thus,

$$f(([x_1]_m, [y_1]_d) + ([x_2]_m, [y_2]_d)) = ([(x_1 + x_2) + (y_1 + y_2)sa']_a, [(x_1 + x_2) - (y_1 + y_2)tb']_b) \tag{5}$$

We can simplify the expression in equation (5) using the associative and commutative properties of addition in $\mathbb{Z}$ and proposition 1.4.2:

$$[(x_1+x_2)+(y_1+y_2)sa']_a = [x_1+y_1sa'+x_2+y_2sa']_a = [x_1+y_1sa']_a + [x_2+y_2sa']_a \quad (6)$$

$$[(x_1+x_2)-(y_1+y_2)tb']_b = [(x_1+x_2-y_1tb'-y_2tb']_b = [x_1-y_1tb']_b + [x_2-y_2tb']_b \quad (7)$$

Equations (6) and (7) imply
$f(([x_1]_m,[y_1]_d)+([x_2]_m,[y_2]_d)) = ([x_1+y_1sa']_a+[x_2+y_2sa']_a, [x_1-y_1tb']_b+[x_2-y_2tb']_b) =$
$([x_1+y_1sa']_a, [x_1-y_1tb']_b)+([x_2+y_2sa']_a, [x_2-y_2tb']_b) = f(([x_1]_m,[y_1]_d))+f(([x_2]_m,[y_2]_d))$.
(one-to-one) To show f is one-to-one, we can use proposition 3.4.4. Suppose
$f(([x]_m,[y]_d)) = ([0]_a,[0]_b)$. Then,

$[x+ysa']_a = [0]_a$ and $[x-ytb']_b = [0]_b$ implies $x+ysa' = la$ and $x-ytb' = kb$ for some $l,k \in \mathbb{Z}$.

Thus, $x = la - ysa'$ and $x = ytb' + kb$ so

$$\begin{aligned}
la - ysa' &= ytb' + kb \\
ytb' + ysa' &= la - kb \\
ytb'd + ysa'd &= lad - kbd && \text{obtained by multiplying by } d \\
ytb + ysa &= lad - kbd && b'd = b \text{ and } a'd = a \\
y(tb+sa) &= lad - kbd \\
y(d) &= lad - kbd && tb + sa = d \\
y &= la - kb && d \neq 0, \text{ so we can divide by d}
\end{aligned}$$

Thus, y is a linear combination of a and b. By theorem 1.1.6, this implies $d|y$. Thus, $y \equiv 0 \pmod{d}$. So, $y = dc$ for some $c \in \mathbb{Z}$. Then, since $x + ysa' \equiv 0 \pmod{a}$ and $x + ysa' = x + dcsa' = x + cs(da') = x + csa$. We have $csa \equiv 0 \pmod{a}$ so $x \equiv 0 \pmod{a}$. From page 22 of Beachy, we know $ab = \gcd(a,b)\text{lcm}[a,b]$. Thus, $md = ab$. Since $|\mathbb{Z}_m \times \mathbb{Z}_d| = md = ab = |\mathbb{Z}_a \times \mathbb{Z}_b|$ and because we've show f is one-to-one, proposition 2.1.8 implies f is onto. Hence, f is an isomorphism. □

Exercise 3.5.3: Give the subgroup diagrams of the groups $\mathbb{Z}_{24}$ and $\mathbb{Z}_{36}$

($\mathbb{Z}_{24}$). Note $|\mathbb{Z}_{24}| = 24$ and $\langle 1 \rangle = \mathbb{Z}_{24}$. By corollary 3.5.4(b), if H is a subgroup of $\mathbb{Z}_{24}$ then $H = \langle k \rangle$ for some divisor of 24. So the subgroups of $\mathbb{Z}_{24}$ are $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 12 \rangle$. Also, 24 divides itself so $\langle 24 \rangle = \langle 0 \rangle$ is a subgroup of $\mathbb{Z}_{24}$. Next by corollary 3.5.4(c) since $3|6$, $6|12$, and $12|24$; $4|12$, $12|24$; $2|4$, $4|8$, $8|24$; and $2|6$, $6|12$, and $12|24$ we must have the following containments:

$$\langle 3 \rangle \supseteq \langle 6 \rangle \supseteq \langle 12 \rangle \supseteq \langle 24 \rangle\,;\ \langle 2 \rangle \supseteq \langle 4 \rangle \supseteq \langle 8 \rangle \supseteq \langle 24 \rangle\,;\ \langle 4 \rangle \supseteq \langle 12 \rangle \supseteq \langle 24 \rangle \text{ and } \langle 2 \rangle \supseteq \langle 6 \rangle \supseteq \langle 12 \rangle \supseteq \langle 24 \rangle$$

Therefore we have the following subgroup diagram:

$$\begin{tikzcd}
& \mathbb{Z}_{24} \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 3 \rangle \arrow[d, dash] & & \langle 2 \rangle \arrow[dll, dash] \arrow[d, dash] \\
\langle 6 \rangle \arrow[d, dash] & & \langle 4 \rangle \arrow[dll, dash] \arrow[d, dash] \\
\langle 12 \rangle \arrow[dr, dash] & & \langle 8 \rangle \arrow[dl, dash] \\
& \langle 0 \rangle &
\end{tikzcd}$$

($\mathbb{Z}_{36}$). Note $|\mathbb{Z}_{36}| = 36$ and $\langle 1 \rangle = \mathbb{Z}_{36}$. By corollary 3.5.4(b), if H is a subgroup of $\mathbb{Z}_{36}$ then $H = \langle k \rangle$ for some divisor of 36. So the subgroups of $\mathbb{Z}_{36}$ are $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 9 \rangle, \langle 12 \rangle, \langle 18 \rangle$. Also, 36 divides itself so $\langle 36 \rangle = \langle 0 \rangle$ is a subgroup of $\mathbb{Z}_{36}$. Next by corollary 3.5.4(c) since $3|6$, $6|12$, and $12|36$; $3|6$, $6|18$, $18|36$; $3|9$, $9|18$, $18|36$; $2|4$, $4|12$, $12|36$; $2|6$, $6|12$, $12|36$; and $2|6$, $6|12$, and $12|24$ we must have the following containments: $\langle 3 \rangle \supseteq \langle 6 \rangle \supseteq \langle 18 \rangle \supseteq \langle 0 \rangle\,; \langle 3 \rangle \supseteq \langle 6 \rangle \supseteq \langle 12 \rangle \supseteq \langle 0 \rangle\,; \langle 3 \rangle \supseteq \langle 9 \rangle \supseteq \langle 18 \rangle \supseteq \langle 0 \rangle\,;\ \langle 2 \rangle \supseteq \langle 4 \rangle \supseteq \langle 12 \rangle \supseteq \langle 0 \rangle\,; \langle 2 \rangle \supseteq \langle 6 \rangle \supseteq \langle 12 \rangle \supseteq \langle 0 \rangle\,;$ and $\langle 2 \rangle \supseteq \langle 6 \rangle \supseteq \langle 18 \rangle \supseteq \langle 0 \rangle$ Therefore we have the following subgroup diagram:

$$
\begin{tikzcd}
& & \mathbb{Z}_{36} \arrow[dl, dash] \arrow[dr, dash] & & \\
& \langle 2\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 3\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 4\rangle \arrow[dr, dash] & & \langle 6\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 9\rangle \arrow[dl, dash] \\
& \langle 12\rangle \arrow[dr, dash] & & \langle 18\rangle \arrow[dl, dash] & \\
& & \langle 0\rangle & &
\end{tikzcd}
$$

Exercise 3.5.13: Show that in a finite cyclic group of order n, the equation $x^m = e$ has exactly m solutions, for each positive integer m that is a divisor of n.

Proof. By theorem 3.5.2, since $|G| = n$ and G is cyclic, $G \cong \mathbb{Z}_n$. So, we will work in $\mathbb{Z}_n$. If $x^m = e$ in $\mathbb{Z}_n$, then $[mx]_n = [0]_n$. Assume $m|n$. Then, $n = dm$ for some $d \in \mathbb{Z},\ d \neq 0$. To show there exists exactly m such $x \in \mathbb{Z}_n$, we will show
$\{[x]_n : [mx]_n = [0]_n\} = \{[kd]_n \ : \ k \in \mathbb{Z}_m\}$. Let $y \in \{[x]_n : [mx]_n = [0]_n\}$ so $0 \leq y < n$.
Then, $my \equiv 0 \pmod{n}$ which implies $my = ln$. Let l be the smallest positive integer such that $my = ln$. Since $n = dm$ we have $my = ldm$ and so $y = ld$. Since $0 \leq y < n$,
$0 \leq my < mn$ and $0 \leq my < mdm$. Further $0 \leq y < dm$. Since $y = ld$ we have
$0 \leq ld < dm$ so $0 \leq l < m$. Thus, $y = ld$ for $l \in \mathbb{Z}_m$ which implies $y \in \{[kd]_n \ : \ k \in \mathbb{Z}_m\}$.
Next, suppose $y \in \{[kd]_n \ : \ k \in \mathbb{Z}_m\}$. Then, $y \equiv kd \pmod{n}$ for $0 \leq k < m$. Equivalently, $my \equiv mkd \pmod{n}$ so $my \equiv k(dm) \pmod{n}$. Sine $k(dm) = k(n)$ and $k(n) \equiv 0 \pmod{n}$ we have $my \equiv 0 \pmod{n}$. Thus, $y \in \{[x]_n : [mx]_n = [0]_n\}$.
Hence, $\{[x]_n : [mx]_n = [0]_n\} = \{[kd]_n \ : \ k \in \mathbb{Z}_m\}$. We claim the number of elements in
$\{[kd]_n \ : \ k \in \mathbb{Z}_m\}$ is m. If there weren't m elements then there must exists some
$k_1, k_2 \in \mathbb{Z}_m$ such that $k_1 d \equiv k_2 d \pmod{n}$, but $k_1 \not\equiv k_2 \pmod{m}$. Thus, $k_1 d = k_2 d + bn$ for some $b \in \mathbb{Z}$. Therefore, $k_1 d = k_2 d + b(dm)$ so $k_1 = k_2 + bm$ which implies $k_1 \equiv k_2 \pmod{m}$.
Thus, there are m elements in the set $\{[kd]_n \ : \ k \in \mathbb{Z}_m\}$ which is equal to the set
$\{[x]_n : [mx]_n = [0]_n\}$. Thus, there are exactly m integers such that $mx \equiv 0 \pmod{n}$.

Therefore, since $G \cong \mathbb{Z}_n$, the equation $x^m = e$ has exactly m solutions for each positive integer m that is divisor of n. $\square$

Exercise 3.5.16: Let G be any group with no proper, nontrivial subgroups, and assume that $|G| > 1$. Prove that G must be isomorphic to $\mathbb{Z}_p$ for some prime p.

Proof. Let G be any group with no proper, nontrivial subgroups, and assume that $|G| > 1$. Then, $|G| \geq 2$ so G contains an identity element, e, and some other element $g \neq e$. By proposition 3.2.6(a), $\langle g \rangle$ is a subgroup of G. Since G has no proper, nontrivial subgroups, and because $g \neq e$, $\langle g \rangle = G$. Thus, G is cyclic. Suppose $|G| = \infty$. Then, by theorem 3.5.2(a), $G \cong \mathbb{Z}$. However, from page 136 of Beachy, we know $\mathbb{Z}$ has proper subgroups of the form $m\mathbb{Z}$ with $m \in \mathbb{Z}$. Since G has no proper subgroups, $G \ncong \mathbb{Z}$ and so $|G| \neq \infty$. Thus, $|G| = n$. So G is a finite cyclic group. On page 136 of Beachy, we know if $G = \langle g \rangle$ is a finite cyclic group, then for every positive divisor m of n, $\langle g^m \rangle$ is a subgroup of G. If $m \neq 1$ and $m \neq n$, then $\gcd(m, n) = m$ and by proposition 3.5.3, $|\langle g^m \rangle| = \frac{n}{m} < n$. Thus, if $m \neq 1$ and $m \neq n$, $\langle g^m \rangle$ is a proper subgroup of G. Since G does not have proper subgroups, this contradiction implies, $m = 1$ or $m = n$. Hence, $1, n$ are the only divisors of n which implies $n = p$ for some prime number p. Then, by theorem 3.5.2, $G \cong \mathbb{Z}_p$ for some prime p. $\square$

Exercise 3.5.18: Prove that $\sum_{d|n} \varphi(d) = n$ for any positive integer n.

Proof. Suppose n has N divisors. Then, rewrite $\sum_{d|n} \varphi(d) = \sum_{k=1}^{N} \varphi(d_k)$ where all $d_k|n$ are considered. Consider some cyclic group $G = \langle g \rangle$ with $|G| = n$. By Theorem 4(5) of Boyton (Cyclic Group handout), for every divisor d_k of n, G has exactly one subgroup of order d_k. Additionally, by Theorem 4(4) of Boyton, every subgroup of G can be as $\left\langle g^d \right\rangle$ for some $d|n$. Thus, consider the collection $\{H_k \leq G : H_k = \left\langle g^{d_k} \right\rangle, |H_k| = d_k\}_{k=1}^{N}$. Define $\sim$ on G where $a \sim b$ if and only if $\langle a \rangle = \langle b \rangle$. By lemma 0.1 below, we know $\sim$ defines an equivalence relation. Let A_k be the equivalence class of H_k. Then, A_k contains all generators of H_k. From Theorem 4(3) of Boyton, we know g^s generates H_k, $|H_k| = d_k$ if and only if $\gcd(s, d_k) = 1$. Thus, H_k has $\varphi(d_k)$ possible generators. So $|A_k| = \varphi(d_k)$. Since A_k are equivalence classes, $A_k \cap A_j = \emptyset$ for all $k \neq j$. By lemma 0.2 below, $G = \bigsqcup_{k=1}^{N} A_k$; therefore, $|G| = |\bigsqcup_{k=1}^{N} A_k|$. Since $\bigsqcup_{k=1}^{N} A_k$ is a disjoint union, $|\bigsqcup_{k=1}^{N} A_k| = \sum_{k=1}^{N} |A_k| = \sum_{k=1}^{N} \varphi(d_k)$. Also, $|G| = n$, so $\sum_{k=1}^{N} \varphi(d_k) = n$.

Lemma 0.1. *Define $\sim$ on G where $a \sim b$ if and only if $\langle a \rangle = \langle b \rangle$. Then, $\sim$ is an equivalence relation.*

Proof. **(reflexive)** For any element $a \in G$, $\langle a \rangle = \langle a \rangle$, so $a \sim a$.
(symmetric) For any $a, b \in G$, if $a \sim b$, then $\langle a \rangle = \langle b \rangle$. Thus, $\langle b \rangle = \langle a \rangle$ so $b \sim a$.
(transitive) Suppose for $a, b, c \in G$, $a \sim b$ and $b \sim c$. Then, $\langle a \rangle = \langle b \rangle$ and $\langle b \rangle = \langle c \rangle$ so $\langle a \rangle = \langle c \rangle$. Thus, $a \sim c$. $\square$

Lemma 0.2. $G = \bigsqcup_{k=1}^{N} A_k$.

Proof. First, show $G \subseteq \bigsqcup_{k=1}^{N} A_k$. Let $g \in G$. Then $\langle g \rangle \leq G$ and since $1|n$ we have $\langle g \rangle \in \{H_k \leq G : H_k = \langle a^{d_k} \rangle, |H_k| = d_k\}_{k=1}^{N}$. Thus, $\langle g \rangle = H_1 = A_1$ Thus, $g \in \bigsqcup_{k=1}^{N} A_k$.
Next, show $G \supseteq \bigsqcup_{k=1}^{N} A_k$. Let $a \in \bigsqcup_{k=1}^{N} A_k$. Then $a \in A_k$ for some k. For all k, $A_k \leq G$, so $a \in G$. $\square$

$\square$

Exercise 3.5.19: Let $n = 2^k$ for $k > 2$. Prove that $\mathbb{Z}_n^\times$ is not cyclic.

Proof. Let $n = 2^k$ for $k > 2$. Then, $|\mathbb{Z}_n^\times| = 2^k > 4$. Notice $n > 4$ implies $\frac{n}{2} + 1 > 1$ and $\frac{n}{2} - 1 > 1$ as well as:

$$n+4 < n+n = 2n; \quad n < 2n-4; \quad \frac{n}{2} < n-2; \quad \frac{n}{2}+1 < n-1 \text{ and similarly, } \frac{n}{2} < n; \quad \frac{n}{2}-1 < n-1.$$

Thus, $1, \frac{n}{2} \pm 1 \in \mathbb{Z}_n^\times$. Notice $\frac{n}{2} \pm 1, n-1$ have order 2 in $\mathbb{Z}_n^\times$:

$$\begin{aligned}
(\tfrac{n}{2}+1)^2 &\equiv \left(\tfrac{2^k}{2}\right)^2 + 2\left(\tfrac{2^k}{2}\right) + 1 &&\equiv 2^k 2^{k-1} + 2^k + 1 &&\equiv 1 \pmod{n} \\
(\tfrac{n}{2}-1)^2 &\equiv \left(\tfrac{2^k}{2}\right)^2 - 2\left(\tfrac{2^k}{2}\right) + 1 &&\equiv 2^k 2^{k-1} - 2^k + 1 &&\equiv 1 \pmod{n} \\
& (n-1)^2 &&\equiv n^2 - 2n + 1 &&\equiv 1 \pmod{n}
\end{aligned}$$

Because $n > 4$, $1 \neq \frac{n}{2} + 1 \neq \frac{n}{2} - 1 \neq n - 1$. From above, we know in $\mathbb{Z}_n^\times$, $o(\frac{n}{2} + 1) = o(\frac{n}{2} - 1) = o(n - 1) = 2$. So we have three distinct elements of order 2. Suppose $\mathbb{Z}_n^\times$ is cyclic. Then, by theorem 3.5.2(b), $\mathbb{Z}_n^\times \cong \mathbb{Z}_n$. Since $\mathbb{Z}_n^\times$ has even order, $|\mathbb{Z}_n| = 2l$ for some $l \in \mathbb{Z}^+$. However, by the lemma below, $\mathbb{Z}_n$ has exactly one element of order 2 where $\mathbb{Z}_n^\times$ has at least three. By proposition 3.4.3, isomorphisms preserve order. Thus, $\mathbb{Z}_n^\times \ncong \mathbb{Z}_n$ which implies $\mathbb{Z}_n^\times$ is not cyclic.

Lemma 0.3. *$\mathbb{Z}_{2l}$ has exactly one element of order 2.*

Proof. Note l is an element of order 2: $l + l \equiv 0 \pmod{2l}$. If there exists $g \in \mathbb{Z}_{2l}$ with $l \neq g$ and $g \neq 0$ (since 0 has order 1) such that $2g \equiv 0 \pmod{2l}$. Then $g \equiv 0$ (mod l implies $g = hl$ for some $h \in \mathbb{Z}$. But, $g \in \mathbb{Z}_{2l}$ so $0 < g < 2l$ and so $0 < hl < 2l$ implies $0 < h < 2$ so $h = 1$ and $l = g$. Thus, there exists exactly one element of order 2 in $\mathbb{Z}_{2l}$. □

□

Exercise 3.5.20: Let G be a group with p^k elements, where p is a prime number and $k \geq 1$. Prove that G has a subgroup of order p.

Proof. Let G be a group with p^k elements, where p is a prime number and $k \geq 1$. Then, $|G| = p^k$. By Lagrange's Theorem, the order of any element in G must divide the order of G. So for any $g \in G$ with $g \neq e$, $|g| = p^l$ for $1 \leq l \leq k$. If $|g| = p$, then $\langle g \rangle$ is a subgroup of G of order p. If $|g| = p^l$ for $2 \leq p \leq k$, then consider $h = g^{p^{l-1}}$. Since p^l is the smallest integer, t, such that $g^t = e$, $p^{l-1} < p^l$ implies $g^{p^{l-1}} \neq e$. Notice $h = (g^p)^{l-1} = (g^{p^l p^{-1}}) = (g^{p^l})^{p^{-1}} = e^{p^{-1}} = e^{-p}$. Therefore $h^p = (e^{-p})^p = e^{\frac{1}{p} \cdot p} = e^1 = e$. So the order of h must divide p. Since $h \neq e$, $|h| = p$ so $\langle h \rangle$ is a subgroup of G of order p. □