2.3

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

$\langle 1 \rangle = \{1\}$

$\langle r \rangle = \{1, r, r^2, r^3\}$

$\langle r^2 \rangle = \{1, r^2\}$

$\langle r^3 \rangle = \{1, r^3, r^2, r\}$

$\langle s \rangle = \{1, s\}$

$\langle sr \rangle = \{1, sr\}$

$\langle sr^2 \rangle = \{1, sr^2\}$

$\langle sr^3 \rangle = \{1, sr^3\}$

We say in class that $H = \{1, r^2, s, sr^2\}$ is a non-cyclic subgroup of D_8.

---

(12) (a) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$

$$\left.\begin{array}{l} \langle (\bar{0},\bar{0}) \rangle = \{(\bar{0},\bar{0})\} \\ \langle (\bar{0},\bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{0},\bar{1})\} \\ \langle (\bar{1},\bar{0}) \rangle = \{(\bar{0},\bar{0}), (\bar{1},\bar{0})\} \\ \langle (\bar{1},\bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{1},\bar{1})\} \end{array}\right\}$$

Hence $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no generators.

(12) (b) You try. See part (c) below.

(c) Let $(m,n) \in \mathbb{Z} \times \mathbb{Z}$.

<u>Case 1: $(m,n) = (0,0)$</u>

Then, $\langle (m,n) \rangle = \{(0,0)\} \neq \mathbb{Z} \times \mathbb{Z}$.

<u>Case 2: $m \neq 0$, $n = 0$</u>

Then, $\langle (m,n) \rangle = \{\ldots, (-2m,0), (-m,0), (0,0), (m,0), (2m,0), \ldots\}$

Then, $(0,1) \notin \langle (m,n) \rangle$. Hence, $\langle (m,n) \rangle \neq \mathbb{Z} \times \mathbb{Z}$.

<u>Case 3: $m = 0$, $n \neq 0$.</u> As above, $(1,0) \notin \langle (m,n) \rangle$.

Hence, $\langle (m,n) \rangle \neq \mathbb{Z} \times \mathbb{Z}$.

<u>Case 4: $m \neq 0$, $n \neq 0$.</u> Then,

$\langle (m,n) \rangle = \{\ldots, (-2m,-2n), (-m,-n), (0,0), (m,n), (2m,2n), \ldots\}$

Note that $(1,0) \notin \langle (m,n) \rangle$. So, $\langle (m,n) \rangle \neq \mathbb{Z} \times \mathbb{Z}$.

Therefore, $\mathbb{Z} \times \mathbb{Z}$ has no generators.

(13) (a) $\mathbb{Z}$ is cyclic and $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic (see problem 12).

(b) Suppose $\frac{m}{n} \in \mathbb{Q}$ with $m, n \neq 0$. Then, $\frac{m}{n}$ has infinite order. since

$$\underbrace{\frac{m}{n} + \dots + \frac{m}{n}}_{k \text{ times}} = \frac{km}{n} \neq 0$$

for any $k > 0$.

However, $(0, \bar{1}) \in \mathbb{Q} \times \mathbb{Z}_2$ and $(0, \bar{1}) + (0, \bar{1}) = (\bar{0}, \bar{0})$. So, $(0, \bar{1})$ has order 2.

Thus, $\mathbb{Q} \not\cong \mathbb{Q} \times \mathbb{Z}_2$ because all non identity elements of $\mathbb{Q}$ have infinite order while $(0, \bar{1})$ is not the identity of $\mathbb{Q} \times \mathbb{Z}_2$ and it has order 2.

(26) I'm rephrasing this problem.

Let $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ have order n.

Define $\sigma_a : G \to G$ with $\sigma_a(g^i) = g^{ai}$.

(a) Let $i, j \in \mathbb{Z}$. Then $\sigma_a(g^i g^j) = \sigma_a(g^{i+j}) =$
$= g^{a(i+j)} = g^{ai} g^{aj} = \sigma_a(g^i)\sigma_a(g^j)$. Hence
σ_a is a homomorphism.

Since $|G|$ is finite, σ_a is 1-1 iff σ_a is onto. By Prop 6, g^a generates G iff $\gcd(a,n)=1$. Note that

$$\text{im}(\sigma_a) = \sigma_a(G) = \{1, g^a, g^{2a}, g^{3a}, \ldots, g^{a(n-1)}\} =$$
$$= \{1, g^a, (g^a)^2, (g^a)^3, \ldots, (g^a)^{n-1}\}.$$

If $\gcd(a,n)=1$, then $\langle g^a \rangle = G$ and so g^a has order n and $\text{im}(\sigma_a) = \{1, g^a, (g^a)^2, \ldots, (g^a)^{n-1}\} = \langle g^a \rangle = G$. Thus, σ_a is onto and 1-1.

If $\gcd(a,n) \neq 1$, then $G \neq \langle g^a \rangle$ and so
$\text{im}(\sigma_a) = \{1, g^a, (g^a)^2, \ldots, (g^a)^{n-1}\} \neq G$.
Thus, σ_a is not onto and not 1-1.

(b) Suppose $a, b \in \mathbb{Z}$. By the division algorithm, $b-a = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < n$.

Note that

$$\sigma_a = \sigma_b \text{ iff } \sigma_a(g) = \sigma_b(g) \text{ iff } g^a = g^b$$
$$\text{iff } g^{b-a} = 1 \text{ iff } g^{nq+r} = 1 \text{ iff } g^r = 1$$
$$\text{iff } r = 0 \text{ (since } n = \text{order}(g)) \text{ iff}$$
$$b - a = nq \text{ iff } b \equiv a \pmod{n}.$$

(c) Let $\sigma : G \to G$ be an automorphism of G. Let $g^a = \sigma(g)$. Then, $\sigma(g^i) = \sigma(g)^i$
$= (g^a)^i = g^{ai} = \sigma_a(g^i)$.

(d) $\boxed{\text{Let } i \in \mathbb{Z}}$ $\sigma_{ab}(g^i) = (g^i)^{ab} = (g^{ib})^a = \sigma_a(g^{ib})$

$$= \sigma_a(\sigma_b(g^i)) = (\sigma_a \circ \sigma_b)(g^i).$$