Abstract Algebra

Solutions of Quiz 1

1.

a) Associativity is inherited from $\mathbb{Z}$. We need to check
(1) Closure: For $a, b \in \mathbb{Z}_{13}^*$, $a \cdot b \neq 0 \Rightarrow a \cdot b \in \mathbb{Z}_{13}^*$
(2) Identity: $\overline{1} \in \mathbb{Z}_{13}^*$ and $\overline{1} \cdot x = x = x \cdot \overline{1}$ for all $x \in \mathbb{Z}_{13}^*$
(3) Inverse:

$$\overline{1} \cdot \overline{1} = \overline{1}, \overline{2} \cdot \overline{7} = \overline{14} = \overline{1}, \overline{3} \cdot \overline{9} = \overline{27} = \overline{1}, \overline{4} \cdot \overline{10} = \overline{40} = \overline{1},$$
$$\overline{5} \cdot \overline{8} = \overline{40} = \overline{1}, \overline{6} \cdot \overline{11} = \overline{66} = \overline{1}, \overline{12} \cdot \overline{12} = \overline{144} = \overline{1}$$

$\Rightarrow \langle \mathbb{Z}_{13}^*, \cdot \rangle$ is a group.

b) False: S_3 is a counterexample.

$$|S_3| = 6 \text{ but } (123)(12) = (13) \neq (23) = (12)(123)$$

c) True.
(1) Closure: For $x, y \in \mathbb{R}\backslash\{-1\}$

$$x \circ y = x + y + xy$$
$$= (x+1)(y+1) - 1 \neq -1 \text{ since } x, y \neq -1$$
$$\Rightarrow x \circ y \in \mathbb{R}\backslash\{-1\}$$

(2) Associativity: Let $x, y, z \in \mathbb{R}\backslash\{-1\}$

$$(x \circ y) \circ z = (x + y + xy) \circ z$$
$$= x + y + xy + z + xz + yz + xyz$$

$$x \circ (y \circ z) = x \circ (y + z + yz)$$
$$= x + y + z + yz + xy + xz + xyz$$
$$\Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$$

(3) Identity: Let $x \in \mathbb{R}\backslash\{-1\}$

$$x \circ 0 = x + 0 + 0 \cdot x = x = 0 \circ x$$

(4) Inverse: Let $x \in \mathbb{R}\backslash\{-1\}$

$$0 = x \circ x^{-1} = x + x^{-1} + x \cdot x^{-1}$$
$$\Rightarrow x^{-1} = \frac{-x}{1+x}$$

$\Rightarrow \langle \mathbb{R}\backslash\{-1\}, \circ \rangle$ is a group.

d) False: $|\mathbb{Z}_4| = 4 = |\mathbb{Z}_2 \times \mathbb{Z}_2|$. But $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ since $\overline{1} \in \mathbb{Z}_4$ has order 4, but there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4.

e) First we are going to show G is a group. The associativity is inherited from the group of all 2×2 matrix.
(1) Closure: Let $A, B \in G$, det(AB)=det(A)det(B)$\neq 0 \Rightarrow AB \in G$
(2) Identity: $I_2 \in G$ since det(I_2)$= 1 \neq 0$

(3) Inverse: For $A \in G$, A is invertible implies A^{-1} is invertible since $(A^{-1})^{-1} = A$

By (1)(2)(3), G is a group.

Last, we are going to show G is not abelian. Consider $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \in G$ but

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix} \neq \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

$\Rightarrow G$ is not abelian.

2. Lemma: If a group G with $|G| = p$ for some prime p, then G is cyclic. In particular, G is abelian.

<proof of lemma>:

Let $a \in G$ and $a \neq e$, let $H = \langle a \rangle$. By Lagrange theorem, $|H| \mid |G| = p$, now $H \neq \{e\}$, hence $|H| = p$, we have $\langle a \rangle = G$. Thus G is cyclic, hence abelian.

Now the group of order 1 is $\{e\}$ is abelian. The group of order $2, 3, 5$ is abelian by the lemma. We only need to show the group of order 4 is abelian.

Suppose $|G| = 4$, if G is cyclic, then we done. If G is not cyclic, then G contains no element of order 4. Suppose the three non-identity elements in G are a, b, c, from Lagrange theorem, we know the order of a, b, c are 2.(i.e., $a^2 = b^2 = c^2 = e$). And $a \cdot b$ must be c since if $a \cdot b = e$ (resp. $a \cdot b = a$,$a \cdot b = b$), then $b = a^{-1} = a$ (resp. $b = e$, $c = e$) a contradiction. Similarly, $b \cdot a = c$, $a \cdot c = c \cdot a = b$, $b \cdot c = c \cdot b = a$, we have the following table:

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

Note that if G is not cyclic, then we have only one way to fill the table, thus, all group of order 4 is abelian.

3. Let $G = \{e, a, a^2, \cdots, a^{n-1}\}$, the number of generators is equal to $\#\{m | 1 < m < n, \gcd(m, n) = 1\} = \phi(n)$, since if $\gcd(i, n) = 1$, then $1 = is + nt$ for some $s, t \in \mathbb{Z}$, thus $g^1 = g^{is+nt} = g^{is}g^{nt} = g^{is}$

$\Rightarrow g \in \langle g^i \rangle$

$\Rightarrow \langle g^i \rangle = G$

If $\gcd(i, n) = d > 1$, then exists $s, t \in \mathbb{Z}$ such that $i = sd, n = td$ with $s, t < n$.

Now $(g^i)^t = g^{it} = g^{sdt} = g^{sn} = 1$

$\Rightarrow |\langle g^i \rangle| < n = |G|$

$\Rightarrow \langle g^i \rangle \neq |G|$