EXERCISE 1

We have $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ and $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. We get the following tables:

$\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$\times$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

EXERCISE 2

We prove that $G = (\mathbb{Q}^*, *)$ is a group.

(1) associativity: for $a, b, c \in \mathbb{Q}^*$ we have

$$a * (b * c) = a * \frac{bc}{2} = \frac{a\frac{bc}{2}}{2} = \frac{abc}{4}$$

$$(a * b) * c = \frac{ab}{2} * c = \frac{\frac{ab}{2}c}{2} = \frac{abc}{4}$$

(2) The identity is 2 since $a * 2 = \frac{2a}{2} = a = 2 * a$.

(3) If $a \in \mathbb{Q}^*$ then $a^{-1} = \frac{4}{a}$.

EXERCISE 3

(1) We prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$.
   (a) Sufficiency. Suppose that $(ab)^2 = a^2b^2$, it means that $abab = aabb$. Multiply both sides by a^{-1} on the left and by b^{-1} on the right.
   (b) Necessity. If now $ab = ba$ then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = aabb$.

(2) To answer the second question one just need to notice that $\varphi : a \mapsto a^2$ is a morphism if and only if $\varphi(ab) = \varphi(a)\varphi(b)$ (i.e. $(ab)^2 = a^2b^2$).

EXERCISE 3

(1) for $n = 1$ we have $aba^{-1} = ab^1a^{-1}$.

(2) If now $(aba^{-1})^n = ab^na^{-1}$ the we have

$$(aba^{-1})^{n+1} = (aba^{-1})^n(aba^{-1}) = (ab^na^{-1})(aba^{-1}) = (ab^n(a^{-1}a)ba^{-1}) = ab^{n+1}a^{-1}$$

EXERCISE 4

We prove that $G = \mathbb{R}^* \times \mathbb{R}$ is a group under the multiplication defined by

$$(a, b)(c, d) = (ac, ad + b)$$

(1) It is easy though tedious to check associativity.

(2) The identity is given by $(1, 0)$

(3) If $(a, b) \in G$ then $(a, b)^{-1} = (\frac{1}{a}, -\frac{b}{a})$.

This group is not commutative. For instance we have $(1, 2)(2, 1) = (2, 3)$ and $(2, 1)(1, 2) = (2, 5)$.

EXERCISE 5

Let G be a group and $a, b \in G$ with $ab = ba$.

(1) Let $n = o(a)$ and $k = o(b)$. Then $(ab)^{nk} = a^{nk}b^{nk} = (a^n)^k(b^k)^n = 1$, hence $o(ab)|o(a)o(b)$. By using the very same argument, it is easy to see that under the same hypotheses we have $o(ab)|lcm(o(a), o(b))$.

(2) Using the previous question, we know that $m = o(ab)|lcm(o(a), o(b))$. By definition of the order, we have $(ab)^m = e$ which leads to $a^m = b^{-m}$. But $< a > \cap < b >= e$ and thus it follows that $a^m = b^m = e$. Hence $lcm(o(a), o(b))|o(ab)$.

(3) Assume that $ab = ba$ and that $o(a)$ and $o(b)$ are coprime. If $< a > \cap < b >= c \neq e$, we see that $o(c)|o(a)$ and $o(c)|o(b)$ which contradicts the hypothesis.

Hence $< a > \cap < b >= e$ and the previous question enables to conclude.

(4) think of a symmetric group.