Algebra II. Exercise 5.
Solutions.

1. First we prove that φ is well defined. Suppose $gH = \bar{g}H \in \mathcal{A}$. Then $\bar{g} = gh$ for some $h \in H$ and

$$\varphi(\bar{g}H) = H\bar{g}^{-1} = H(gh)^{-1} = Hh^{-1}g^{-1} = Hg^{-1} = \varphi(gH).$$

Then we prove injectivity. Suppose $\varphi(gH) = \varphi(\bar{g}H)$, that is, $Hg^{-1} = H\bar{g}^{-1}$. Then $\bar{g}^{-1} = hg^{-1}$ for some $h \in H$ and thus $\bar{g} = gh^{-1}$. From this it follows that $\bar{g}H = gh^{-1}H = gH$, which proves injectivity.
To prove surjectivity, let $H\bar{g} \in \mathcal{B}$. When we choose $g = \bar{g}^{-1}$, we have $\varphi(gH) = Hg^{-1} = H(\bar{g}^{-1})^{-1} = H\bar{g}$, which proves surjectivity.

2. a) Consider the group S_3 and subgroups $H = \{(1), (12)\}$ and $K = \{(1), (13)\}$. Then $HK = \{(1), (12), (13), (132)\}$, which is not a subgroup of S_3. This can be seen in several ways: HK doesn't contain the inverse of (132); also $(132)(12) = (23) \notin HK$; also S_3 cannot have a subgroup of order 4.

b) Consider again S_3 and now the subgroups $H = \{(1), (123), (132)\}$ and $K = \{(1), (12)\}$. Now H is a normal subgroup of S_3 (which can be verified directly, but also follows from the fact that H has index 2 in S_3). Hence by Lemma 4.1 we know that $HK \leq S_3$, and since HK has at least 4 elements, it has to be the whole group S_3. Clearly $H \cap K = \{(1)\}$. The groups S_3 and $H \times K$ are not isomorphic, since S_3 is not Abelian, but $H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ is.

3. "(i)⇒(ii)": Let $g \in G$, $g \neq e$. Then the subgroup generated by g is not trivial, so by assumption we have $\langle g \rangle = G$, that is, G is a cyclic group. If G were infinite, then by [Häsä-Rämö, Proposition 9.5, p. 126] G would be isomorphic to $(\mathbb{Z}, +)$; this group, however, has non-trivial proper subgroups, for example $2\mathbb{Z}$, so G here cannot be infinite. Thus G is a finite cyclic group, and hence by [Häsä-Rämö, Proposition 9.6, p. 126] it is isomorphic to the group $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{N}$, $n \geq 2$. If n were not a prime number, it would have a representation as a product $n = k \cdot l$, $1 < k, l < n$. Now by [Häsä-Rämö, Proposition 9.16, p. 132] G would have for example subgroups

of order k and l, which is a contradiction with our assumption. Thus n has to be a prime number, and the claim follows.

"(ii)⇒(iii)": Clear.

"(iii)⇒(iv)": If the order of a group is a prime number, the group is cyclic, see [Häsä-Rämö, Proposition 11.16, p. 156], and a cyclic group is always commutative, see [Häsä-Rämö, Proposition 9.2, p. 123]. Moreover $G \neq \{e\}$ and by Lagrange's theorem the only subgroups of G are $\{e\}$ and G, thus the group is simple.

"(iv)⇒(i)": By the definition of a simple group, G is not trivial. If G had a proper non-trivial subgroup, then by commutativity this subgroup would also be normal; this would contradict the assumption that G is simple. Thus condition (i) holds.

4. Suppose $|G| = p^k m,\ k \geq 1$ and p is not a factor of m. By the Sylow theorem the group G has a subgroup H, $|H| = p^k > 1$. Choose $x \in H,\ x \neq e$. Now the order $|\langle x \rangle|$ is a factor of the order $|H|$ and $|\langle x \rangle| \neq 1$, so $\mathrm{ord}(x) = |\langle x \rangle| \in \{p, ..., p^k\}$, that is, $\mathrm{ord}(x) = p^l$ for some $l \in \{1, ..., k\}$. The cyclic group $\langle x \rangle$ has a subgroup corresponding to each factor of its' order p^l, see [Häsä–Rämö, Proposition 9.16, p. 132], especially there exists a subgroup K of order p. In the subgroup K we can find an element, whose order is p: any element $g \in K$, $g \neq e$, generates the subgroup K, that is, $\mathrm{ord}(g) = p$.

5. a) We have that $k \cdot ([1]_m, [1]_n) = ([k]_m, [k]_n) = ([0]_m, [0]_n)$, if and only if k is a common multiple of the numbers m and n. Since $\gcd(m, n) = 1$, the least common multiple of m and n is mn [Häsä–Rämö, Proposition 5.8, p. 81]. Thus the order of the element $([1]_m, [1]_n)$ is the same as the order of the whole group, that is, this element generates the group. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is a cyclic group of order mn, hence it is isomorphic to $\mathbb{Z}_{mn}$, see [Häsä–Rämö, Proposition 9.6, p. 126].

b) The group $\mathbb{Z}_n \times \mathbb{Z}_n$ has (at least) two subgroups of order n, namely $\{[0]_n\} \times \mathbb{Z}_n$ and $\mathbb{Z}_n \times \{[0]_n\}$. The cyclic group $\mathbb{Z}_{n^2}$ has exactly one subgroup of order n, namely $\langle [n]_{n^2} \rangle$, see [Häsä–Rämö, Proposition 9.16, p. 132].
An isomorphism maps subgroups to subgroups and preserves the orders of subgroups, so from the above it follows that the groups are not isomorphic.

6. By Cauchy's Theorem the group G has a subgroup H of order p. Choose $x \in G \setminus H$. Since $x \neq e$, the possible orders for x are p and p^2.

If the order of x is p^2, we have that $\langle x \rangle = G$, and hence G is a cyclic group and thus isomorphic to the group $\mathbb{Z}_{p^2}$.
If the order of x is p, we have $\langle x \rangle \cap H = \{e\}$ (the intersection is a subgroup of H, so it has order 1 or p. It cannot be p, because $x \notin H$, so it has to be 1). From Exercise 5 of last week it follows that G is commutative, hence all subgroups are normal. Thus by Lemma 4.1 the product set $\langle x \rangle H$ is a subgroup. It has order $> p$, so the order must be p^2. Thus $\langle x \rangle H = G$. The assumptions of Proposition 4.2 hold, and we get

$$G \cong \langle x \rangle \times H \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

In the last step we used the fact that any group of order p (p prime) is isomorphic to $\mathbb{Z}_p$.