Department of Mathematics and Statistics
Introduction to Algebraic topology, fall 2013
Exercises 6. Solutions

1. An element x of an abelian group G is called *torsion* element if there exists $n \in \mathbb{Z}, n > 0$ such that $nx = 0$ (where 0 is a neutral element of G). The set of all torsion elements of G is denoted $\operatorname{Tor}(G)$. If $\operatorname{Tor}(G) = \{0\}$, G is called *torsion free.*
a) Prove that $\operatorname{Tor}(G)$ is always a subgroup of G.
b) Show that quotient group $G/\operatorname{Tor}(G)$ is always torsion free.
c) Show that the torsion subgroup $\operatorname{Tor}(\mathbb{R}/\mathbb{Z})$ of the quotient group $\mathbb{R}/\mathbb{Z}$ is $\mathbb{Q}/\mathbb{Z}$.

Solution:
a) Since $1 \cdot 0 = 0$ (or actually $n \cdot 0 = 0$ for all $n > 0$), zero element of G is a torsion element, so $0 \in \operatorname{Tor}(G)$.

Suppose $x, y \in \operatorname{Tor}(G)$. Then there exist integers $n, m > 0$ such that $nx = 0 = my$. It follows that for $k = nm$ we have

$$k(x+y) = kx+ky = (nm)x+(nm)y = m(nx)+n(my) = m\cdot 0+n\cdot 0 = 0.$$

Notice that we are using a lot of "obvious" algebraic laws that need to be proven, like distributivity of multiplication by integers in the group,

$$k(x + y) = kx + ky$$

and "associativity" $(nm)x = n(mx)$. The exact proof of these is left to the reader to verify. In this instance it is enough to know these for positive integers only (but in general we will be using those laws a lot for arbitrary integers). Also the commutativity of the multiplication of integers is used between the lines.

Finally we need to show that whenever $x \in \operatorname{Tor}(G)$, then also $-x \in \operatorname{Tor}(G)$. Let $n > 0$ be such that $nx = 0$. Then

$$n(-x) = -nx = -0 = 0$$

in group G, so also $-x$ is a torsion element. The formula $n(-x) = -nx$ is actually a consequence of the distributive law mentioned above, since

$$n(-x) + nx = n((-x) + x)) = n0 = 0.$$

b) Since $\operatorname{Tor}(G)$ is a subgroup of G (and groups are abelian), we can form the quotient group $G/\operatorname{Tor}(G)$. We need to show that the only torsion element of this group is the neutral element, which in this group is actually the class $\operatorname{Tor}(G)$.

Suppose $\bar{g} = g + \operatorname{Tor}(G)$ is a torsion element. This means that for some $n > 0$ we have that

$$n\bar{g} = \overline{ng} = \bar{0} = \operatorname{Tor}(G).$$

This is equivalent to $ng \in \operatorname{Tor}(G)$. Since ng is a torsion element, there exists $m > 0$ such that $m(ng) = 0$ in G. But this is the same as $(nm)g = 0 \in G$ and since $k = nm$ is an integer, we see that $g \in \operatorname{Tor}(G)$, so $\bar{g} = \bar{0}$ is a zero element of the group $G/\operatorname{Tor}(G)$. Hence the latter is indeed torsion free.

c) Suppose $\bar{x} \in \mathbb{R}/\mathbb{Z}$ is a class of $x \in \mathbb{R}$. Then $\bar{x}$ is a torsion element of $\mathbb{R}/\mathbb{Z}$ if and only if there exists $n \in \mathbb{Z}, n > 0$ such that

$$n\bar{x} = \overline{nx} = \bar{0} = \mathbb{Z},$$

which is equivalent to $nx \in \mathbb{Z}$. This is equivalent to the existence of $m \in \mathbb{Z}$ such that $nx = m$. Hence we have shown that $\bar{x}$ is a torsion element if and only if

$$x = \frac{m}{n}$$

for some $m, n \in \mathbb{Z}$, $n > 0$. But this is equivalent to $x \in \mathbb{Q}$. Hence torsion element of $\mathbb{R}/\mathbb{Z}$ are precisely elements of $\mathbb{Q}/\mathbb{Z}$.

Notice that the quotient group $\mathbb{Q}/\mathbb{Z}$ is **literally** a subset of the quotient group $\mathbb{R}/\mathbb{Z}$. Indeed, by definition element of $\mathbb{Q}/\mathbb{Z}$ is a set of the form

$$q + \mathbb{Q} = \{q + m \mid m \in \mathbb{Z}\}$$

and such a set is in particular an element of $\mathbb{R}/\mathbb{Z}$ (by definition of the quotient group again).

The neutral element is $1 = (1, 0)$. The set of complex numbers of norm 1

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

is a subgroup of $\mathbb{C}^*$. All elements of S^1 can be represented in the form

$$(\cos\alpha, \sin\alpha)$$

where angle α is unique up to a multiply of 2π.

2. For every $n \in \mathbb{N}, n > 0$ we let

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

a) Show that C_n is isomorphic to $\mathbb{Z}_n$ for all $n > 0$.
b) Show that

$$\operatorname{Tor} \mathbb{C}^* = \bigcup_{n>0} C_n$$

c) Consider the mapping $f\colon \mathbb{R} \to \mathbb{C}^*$,

$$f(x) = (\cos 2\pi x, \sin 2\pi x).$$

Show that $f\colon (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ is a homomorphism of abelian groups and use f to prove that the quotient groups $\mathbb{R}/\mathbb{Q}$ and $S^1/\operatorname{Tor}\mathbb{C}^*$ are isomorphic.

Solution: Here we need to recall the multiplication of complex numbers and some of its essential properties.

The set $\mathbb{C}$ of complex numbers is defined to be $\mathbb{R}^2$ i.e. the set of real-valued pairs (x, y). The multiplication of complex numbers is defined by the formula

$$(x, y) \cdot (u, v) = (xu - yv, xv + yu).$$

It can be shown (any standard algebra text or prove-it-yourself) that the set of all **non-zero** complex numbers $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is an abelian group when equipped with this multiplication. The zero element is the complex number $1 = (1, 0)$. The opposite element of complex number $(x, y) \neq 0$ is called inverse element (since we are using multiplicative notation) and denoted $(x, y)^{-1}$, it can be shown that

$$(x, y)^{-1} = (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}).$$

As elements the plane $\mathbb{R}^2$ complex numbers have natural norm $|\cdot|$, which is the standard norm

$$|(x, y)| = \sqrt{x^2 + y^2}.$$

This norm is "compatible" with multiplication, meaning that for all complex numbers z, w we have that

$$|z \cdot w| = |z| \cdot |w|.$$

We also have that $|1| = 1$ (here on the left side complex number 1, on the right side real number 1). These implies that for all $z \neq 0$ we have that

$$1 = |1| = |z \cdot z^{-1}| = |z| \cdot |z^{-1}|,$$

so

$$|z^{-1}| = |z|^{-1}.$$

It follows that the circle

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

is a subgroup of $\mathbb{C}^*$ with respect to the multiplication. As we know from basic mathematics, elements of S^1 can be represented in the form

$$z = (\cos 2\pi\alpha, \sin 2\pi\alpha),$$

where $\alpha \in \mathbb{R}$. Such a representation is not unique, but it is unique up to an integer. In other words for any other $\beta \in \mathbb{R}$ the equation

$$z = (\cos 2\pi\beta, \sin 2\pi\beta)$$

is true if and only if $\alpha - \beta = n$ for some $n \in \mathbb{Z}$.

The mapping $f \colon \mathbb{R} \to S^1$ defined by

$$f(x) = (\cos 2\pi x, \sin 2\pi x)$$

is a surjective **homomorphism** of abelian groups $(\mathbb{R}, +)$ and $(S^1, \cdot)$. This claim is a part of b) but let us prove it now in advance, since it will come in handy in the proof of a) as well. The formulas for the sine and cosine of the sum of two angles gives us that

$$f(x+y) = (\cos 2\pi(x+y), \sin 2\pi(x+y)) =$$

$$= (\cos 2\pi x \cos 2\pi y - \sin 2\pi x \sin 2\pi y, \cos 2\pi x \sin 2\pi y + \sin 2\pi x \cos 2\pi y) =$$

$$= (\cos 2\pi x, \sin 2\pi x) \cdot (\cos 2\pi y, \sin 2\pi y) = f(x)f(y).$$

This proves that f is a homomorphism of groups. It is surjective since every element of S^1 can be written in the form

$$z = (\cos 2\pi\alpha, \sin 2\pi\alpha),$$

where $\alpha \in \mathbb{R}$.

a) Let z be an element of C_n. Then iteration of the formula $|z \cdot w| = |z| \cdot |w|$ for $z = w$ gives

$$|z|^n = |z^n| = |1| = 1,$$

which implies, since $|z|$ is a non-negative real number, that $|z| = 1$ i.e. $z \in S^1$. In particular we can write z in the form

$$z = (\cos 2\pi x, \sin 2\pi x) = f(x)$$

for some $x \in \mathbb{R}$ (unique up to the addition of an integer). Since f was shown to be a homomorphism above, we have that

$$(1, 0) = z^n = f(x)^n = f(nx) = (\cos 2\pi nx, \sin 2\pi nx).$$

This is possible if and only if $2\pi nx = m2\pi$ for some integer $m \in \mathbb{Z}$ i.e. if and only if $x = m/n$. Hence

$$C_n = \{(\cos \frac{2\pi m}{n}, \sin \frac{2\pi m}{n}) \mid m \in \mathbb{Z}\}.$$

Define $\alpha \colon \mathbb{Z} \to S^1$ by

$$\alpha(m) = (\cos \frac{2\pi m}{n}, \sin \frac{2\pi m}{n}).$$

By considerations above the image of α is precisely C_n. Just as we have seen that f is homomorphism, one easily sees, using the formulas for the sine and cosine of the sum of angles, that α is a homomorphism of abelian groups. Since an image of an abelian group w.r.t. a homomorphism is an abelian group itself, we see that C_n is an abelian group.

By isomorphism theorem 7.9. there exists an isomorphism $\bar{\alpha} \colon \mathbb{Z}/\operatorname{Ker}\alpha \to C_n$ of abelian groups. We calculate $\operatorname{Ker}\alpha$. Suppose $m \in \mathbb{Z}$ is such that

$$\alpha(m) = (\cos \frac{2\pi m}{n}, \sin \frac{2\pi m}{n}) = (1, 0).$$

This is possible if and only if $2\pi m/n = k2\pi$ for some $k \in \mathbb{Z}$, which is equivalent to $m = nk$. Hence the kernel of α consists precisely of integers divisible by n, in other words $\operatorname{Ker}\alpha = n\mathbb{Z}$. Hence $\bar{\alpha}$ is an isomorphism between $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ and C_n, which is what we had to prove.

b) The equation

$$\operatorname{Tor}\mathbb{C}^* = \bigcup_{n>0} C_n$$

follows trivially from the definition of the torsion subgroup and groups C_n.

c) We have already seen that $f\colon \mathbb{R} \to \mathbb{C}^*$,

$$f(x) = (\cos 2\pi x, \sin 2\pi x)$$

is a homomorphism between abelian groups $(\mathbb{R}, +)$ and $(\mathbb{C}^*, \cdot)$ and it's image is precisely S^1. By Exercise 1 there exists a quotient subgroup $S^1/\operatorname{Tor}\mathbb{C}^*$.

Let $g = p \circ f\colon \mathbb{R} \to S^1/\operatorname{Tor}\mathbb{C}^*$ be the composition of $f\colon \mathbb{R} \to S^1$ and the canonical projection $p\colon S^1 \to S^1/\operatorname{Tor}\mathbb{C}^*$. Then g is a surjective homomorphism of groups. By Isomorphism Theorem 7.9. g induces an isomorphism

$$\bar{g}\colon \mathbb{R}/\operatorname{Ker} g \to S^1/\operatorname{Tor}\mathbb{C}^*.$$

Next we calculate $\operatorname{Ker} g$. Suppose $x \in \mathbb{R}$. Then

$$\bar{g}(x) = f\bar{(}x) = \bar{1} = \operatorname{Tor}\mathbb{C}^*,$$

which is a zero element of $S^1/\operatorname{Tor}\mathbb{C}^*$ if and only if

$$f(x) = (\cos 2\pi x, \sin 2\pi x) \in \operatorname{Tor}\mathbb{C}^*.$$

By a) and b) we have that

$$\operatorname{Tor}\mathbb{C}^* = \bigcup_{n>0} C_n = \bigcup_{n>0} \{(\cos \frac{2\pi q}{,} \sin \frac{2\pi m}{n}) \mid m \in \mathbb{Z}\} = \{(\cos 2\pi q, \sin\ 2\pi q) \mid q \in \mathbb{Q}\}.$$

In other words

$$\operatorname{Tor}\mathbb{C}^* = \{f(x) \mid x \in \mathbb{Q}\}.$$

Suppose $x \in \mathbb{Q}$. Then, by the last equation, $f(x) \in \operatorname{Tor}\mathbb{C}^*$. Suppose conversely that $f(x) \in \operatorname{Tor}\mathbb{C}^*$. Then, by the same equation, $f(x) = f(q)$ for some $q \in \mathbb{Q}$. This implies that $x - q = m$ for some integer $m \in \mathbb{Z}$, so, $x = q + m \in \mathbb{Q}$. Hence we see that $f(x) \in \operatorname{Tor}\mathbb{C}^*$ if and only if $x \in \mathbb{Q}$. This means precisely that $\operatorname{Ker} g = \mathbb{Q}$. Hence $\bar{g}$ is an isomorphism between $\mathbb{R}/\mathbb{Q}$ and $S^1/\operatorname{Tor}\mathbb{C}^*$.

3. Let A be a set. For every $a \in A$ we define $f_a \colon A \to \mathbb{Z}$ by

$$f_a(x) = \begin{cases} 1, & \text{if } x = a, \\ 0, & \text{otherwise }. \end{cases}$$

a) Prove that $\mathbb{Z}^A$ is an abelian group (with point-wise addition, see lecture notes) and $\mathbb{Z}^{(A)}$ is its subgroup.
b) Prove that

$$\{f_a \mid a \in A\}$$

is a basis of $\mathbb{Z}^{(A)}$.

Solution: a) The addition $+$ in Z^A is defined as following. Suppose $f, g \in Z^A$. We define $f + g \colon A \to \mathbb{Z}$ to be the function such that

$$(f + g)(a) = f(a) + g(a) \text{ for all } a \in A.$$

We need to show that $+$ satisfies the conditions of abelian group.

1) Associativity: Suppose $f, g, h \in \mathbb{Z}^A$. Let $a \in A$ be arbitrary. Then

$$((f+g)+h)(a) = (f+g)(a)+h(a) = (f(a)+g(a))+h(a) =^* f(a)+(g(a)+h(a)) =$$

$$f(a) + (g + h)(a) = (f + (g + h))(a).$$

Notice that in (*) we have used the associativity of the usual addition of integers.
Since $((f + g) + h)(a) = (f + (g + h))(a)$ for all $a \in A$, we have that

$$(f + g) + h = f + (g + h).$$

2) Commutativity: Suppose $f, g \in \mathbb{Z}^A$. Let $a \in A$ be arbitrary. Then

$$(f + g)(a) = f(a) + g(a) =^* g(a) + f(a) = (g + f)(a).$$

Notice that in (*) we have used the commutativity of the usual addition of integers.
Since $(f + g)(a) = (g + f)(a)$ for all $a \in A$, we have that

$$f + g = g + h.$$

3) Zero element of $\mathbb{Z}^A$ is the constant function $0 \colon A \to \mathbb{Z}$ defined by $0(a) = 0$ for all $a \in A$. Indeed, for every $f \in Z^A$ and all $a \in A$ we have that

$$(f + 0)(a) = f(a) + 0(a) = f(a) + 0 = f(a),$$

so $f + 0 = f$.

4) Suppose $f \in \mathbb{Z}^A$. We define $-f \in \mathbb{Z}^A$ by

$$(-f)(a) = -f(a), a \in A.$$

Then, for all $a \in A$ we have that

$$(f + (-f))(a) = f(a) + (-f(a)) =^* 0 = 0(a),$$

so $f + (-f) = 0$. In (*) we have used the definition of the opposite element in the abelian group $\mathbb{Z}$.

Next we show that $\mathbb{Z}^{(A)}$ is a subgroup of $\mathbb{Z}^A$. First of all the support of zero function $0 \in \mathbb{Z}^A$ is the empty set, which is finite, so 0 is finitely supported, in other words $0 \in \mathbb{Z}^{(A)}$.

Suppose $f, g \in \mathbb{Z}^{(A)}$. Then the supports

$$B_f = \{a \in A \mid f(a) \neq 0\},$$

$$B_g = \{a \in A \mid g(a) \neq 0\}$$

are both finite. We claim that

$$B_{f+g} \subset B_f \cup B_g.$$

Suppose $x \notin B_f \cup B_g$. Then $f(a) = 0$ and $g(a) = 0$, so $(f + g)(a) = f(a) + g(a) = 0$. Hence $x \notin B_{f+g}$. Thus, if $x \in B_{f+g}$, then $x \in B_f \cup B_g$. Union of finite sets is finite, so $B_f \cup B_g$ is finite. A subset of a finite set is finite, so B_{f+g} is finite. Hence $f + g \in Z^{(A)}$ whenever $f, g \in Z^{(A)}$.

Finally we notice that for any $f \in \mathbb{Z}^A$

$$B_{-f} = B_f,$$

so if $f \in Z^{(A)}$, then also $-f \in Z^{(A)}$. We have shown that $\mathbb{Z}^{(A)}$ satisfies all the conditions of an abelian group.

b) Suppose $f \in \mathbb{Z}^{(A)}$, then

$$B_f = \{a \in A \mid f(a) \neq 0\}$$

is a finite sum. We claim that

$$f = \sum_{a \in B_f} f(a) f_a.$$

Indeed, if $b \notin B_f$, then

$$f(a) = 0 = \sum_{a \in B_f} f(a) f_a(b).$$

If $b \in B_g$, then

$$f(b) = \sum_{a \in B_f} f(a) f_a(b),$$

because $f_b(b) = 1$ and $f_a(b) = 0$ for all $a \neq b$.

Since

$$f = \sum_{a \in B_f} f(a) f_a$$

we see that in particular the set $\{f_a \mid a \in A\}$ generates the whole group $\mathbb{Z}^{(A)}$ (obviously every element of this set is finitely supported, so conversely the group generated by it must be a subset of $\mathbb{Z}^{(A)}$). It remains to show that this set is linearly independent. Suppose $B = \{a_1, \ldots, a_k\} \subset A$ is a finite subset of A and

$$n_1 a_1 + \ldots + n_k a_k = 0$$

for some integers $n_1, \ldots, n_k \in \mathbb{Z}$. Evaluating this some (both sides are functions!) in a_i for $i = 1, \ldots, k$ we obtain

$$n_i = (n_1 a_1 + \ldots + n_k a_k)(a_i) = 0(a_i) = 0.$$

Since this is true for all $i = 1, \ldots, k$, set A is linearly independent, which is what we had to show.

4. Suppose G is an abelian group and $(H_\alpha)_{\alpha \in \mathcal{A}}$ is indexed collection of abelian groups. Suppose for every $\alpha \in \mathcal{A}$ a homomorphism of abelian groups $f_\alpha \colon G \to H_\alpha$ is given. Prove that then there exists unique homomorphism of groups

$$f \colon G \to \prod_{\alpha \in \mathcal{A}} H_\alpha$$

such that $\mathrm{pr}_\alpha \circ f = f_\alpha$ for all $\alpha \in \mathcal{A}$.

Solution: Suppose $f\colon G \to \prod_{\alpha\in\mathcal{A}} H_\alpha$ is such that $\mathrm{pr}_\alpha \circ f = f_\alpha$ for all $\alpha \in \mathcal{A}$. Suppose $g \in G$ and consider the family

$$f(g) = (h_\alpha)_{\alpha\in\mathcal{A}}.$$

Since $\mathrm{pr}_\alpha \circ f = f_\alpha$ for all $\alpha \in \mathcal{A}$, we have for every fixed $\beta \in \mathcal{A}$ that

$$h_\beta = (\mathrm{pr}_\beta \circ f)(g) = f_\beta(g).$$

Hence

$$f(g) = (f_\alpha(g))_{\alpha\in\mathcal{A}},$$

so the element $f(g)$ is uniquely determined. This proves the uniqueness of f.

To prove uniqueness we define $f\colon G \to \prod_{\alpha\in\mathcal{A}} H_\alpha$ by the formula already deduced above,

$$f(g) = (f_\alpha(g))_{\alpha\in\mathcal{A}}, \text{ for all } g \in G.$$

Then $\mathrm{pr}_\alpha \circ f = f_\alpha$ for all $\alpha \in \mathcal{A}$ by construction. It remains to show that f is a homomorphism of abelian gropus. Let $g, g' \in G$. Then

$$f(g+g') = (f_\alpha(g+g'))_{\alpha\in\mathcal{A}} = (f_\alpha(g)+f_\alpha(g'))_{\alpha\in\mathcal{A}} = (f_\alpha(g))_{\alpha\in\mathcal{A}}+(f_\alpha(g'))_{\alpha\in\mathcal{A}} = f(g)+f(g').$$

Here we have used the fact that every mapping f_α is a homomorphism, as well as the actual definition of the $+$-operation in the direct product $(H_\alpha)_{\alpha\in\mathcal{A}}$.

5. Prove that
a) $\mathbb{Z}_6$ is isomorphic to the direct sum $\mathbb{Z}_2 \oplus \mathbb{Z}_3$,
b) $\mathbb{Z}_4$ is not isomorphic to the direct sum $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
What do you think is the essential difference between those cases responsible for these results? Try to conjecture some general results similar to those special cases (you do not have to prove your conjectures, of course).

Solution: The key is to look at the **order** of elements. The order of an element $g \in G$, where G is an abelian group, is the smallest positive integer $n \in \mathbb{Z}$ such that $ng = 0$ or infinity ∞ if such an integer does not exist. For example 0 is the only element of order 1.

Isomorphism clearly preserve orders of elements. Using this fact we can easily deduce that $\mathbb{Z}_4$ is not isomorphic to the direct sum $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Indeed, every element of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ has order at most 2, since

$$2(x, y) = (2x, 2y) = (0, 0) = 0$$

for all $x, y \in \mathbb{Z}_2$. But in the group $\mathbb{Z}_4$ there exists an element g such that $2g \neq 0$, namely

$$2\bar{1} = \bar{2} \neq 0 \in \mathbb{Z}_4,$$

because 2 is not divisible by 4. Also element $\bar{3} \in \mathbb{Z}_4$ is such that $2\bar{3} \neq 0$. For any homomorphism $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2 \to \mathbb{Z}_4$ we have that

$$0 = f(2g) = f(g + g) = f(g) + f(g) = 2f(g), \text{ for all } g \in \mathbb{Z}_2 \to \mathbb{Z}_2.$$

so the image of this homomorphism cannot contain element $\bar{1}$, hence cannot be surjection.

It is usually easier to prove that some groups are not isomorphic, you just have to find an algebraic property (i.e. property that isomorphisms must preserve) that one group has and the other does not. Let's how we proved b). To prove that two groups are isomorphic, we must actually construct an isomorphism between them. One of the most used tricks is to do this by using the Isomorphism Theorem - it is enough to construct a surjective homomorphism and then quotient out by the kernel. Hence, to prove that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is homeomorphic to $\mathbb{Z}_6$, we will first try to come up with a surjective homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Since all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, this will, in any case, give us an isomorphism $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$ for some $n \in \mathbb{Z}$. If the claim we want to prove is true, we'll be able to have this result for $n = 6$.

Any homomorphism $f\colon \mathbb{Z} \to G$, where G is an arbitrary abelian group, is determined once we know $f(1)$. This is because 1 *generates* $\mathbb{Z}$, so for any $n \in \mathbb{Z}$ we have

$$f(n) = f(n \cdot 1) = nf(1).$$

This implies, that the image of the homomorphism $f\colon \mathbb{Z} \to G$ is a subgroup of G generated on one element $f(1)$. In particular f can be surjective if and only if G is a group generated on one element. Hence first we must find a generator of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Direct broute-force: One way to find a generator is to go through all elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Since there are only six elements, it is possible in practice.

Abstract algebra : You might know from the basic course in algebra that an element $g \in G$ always generates the subgroup, which size is exactly the order of g. This is actually consequence of an isomorphism theorem - we consider homomorphism $f\colon \mathbb{Z} \to G$ given by $f(n) = ng$ and using isomorphism theorem we conclude that f induces an isomorphism $\mathbb{Z}/\operatorname{Ker} f \to G'$, where G' is the subgroup generated by g. If $\operatorname{Ker} f = \{0\}$ this means that the order of g is infinite and G' is isomorphic to $\mathbb{Z}$. If $\operatorname{Ker} \mathbb{Z} = n\mathbb{Z}$ for some $n > 0$, then, by definition of f, the order of g is precisely n and on the other hand G' is isomorphic to $\mathbb{Z}_n$, which has precisely n elements.

If we apply this knowledge to $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, we realise, that the latter group is generated by one element g if and only if this element has order 6. Going through the order of elements we see that for example $(bar1, \bar{1}) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$ has order 6. The considerations above actually show that then $f\colon \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$ defined by

$$f(n) = nbar1, \bar{1})$$

defines an isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, which is what had to be shown.

General Fact: It can be shown that the group $\mathbb{Z}_n \oplus \mathbb{Z}_m$ (which has mn elements) is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are co-primes, i.e. $g.c.d(n, m) = 1$. The proof can be found in texts on basic abstract algebra.

6. a) Suppose A is a linearly independent subset of the abelian group $(\mathbb{Q}, +)$. Prove that A has at most one element.
b) Use a) to prove that $\mathbb{Q}$ is not free.
c) Show also that $\mathbb{Q}$ is not finitely generated.

Solution: a) Enough to prove that if A contains at least two different elements

$$x = m/n, y = k/l,$$

then A cannot be linearly independent. But

$$(nk)x - (ml)y = mk - mk = 0.$$

This combination is non-trivial, since denominators n, l are non-zero and at least one of the nominators m, k must also be non-zero (otherwise $x = y = 0$). Hence A cannot be free.

c) We do c)-first. Suppose $A = \{a_1 = m_1/n_1, a_2 = m_2/n_2, \ldots, a_i = m_i/n_i, \ldots, a_k = m_k/n_k\}$ is a finite subset of $\mathbb{Q}$. We'll show that A cannot generate $\mathbb{Q}$. If it would generate the whole $\mathbb{Q}$, then in particular there would exist integers $l_1, \ldots, l_k$ such that

$$l_1a_1 + l_2a_2 + \ldots + l_ka_k = \frac{1}{2n},$$

where $n = n_1n_2 \cdots n_k$. The sum of the left side can be written in the form

$$\frac{l}{n},$$

where $l \in \mathbb{Z}$. Cancelling out n from both parts of the equations gives us that $1/2$ is an integer l, which is impossible. Hence A cannot generate the whole A.

b) Suppose $\mathbb{Q}$ is free and let A be its basis. By a) A must be at most singleton. However by c) $\mathbb{Q}$ is not finitely generated, so in particular cannot be generated by a singleton (or empty set) A. Contradiction.