GROUPS AND RINGS - PROBLEM SHEET 2
Solutions

1. We prove the following facts.

   (a) for all $k \in \{1, 2, 3, \ldots, n\}$: $(k\ k+1) \in \langle (1\ 2), (1\ 2\ 3\ 4 \ldots\ n) \rangle$;

   (b) for all $k \in \{1, 2, 3, \ldots, n\}$: $(1\ k) \in \langle (1\ 2), (1\ 2\ 3\ 4 \ldots\ n) \rangle$;

   (c) for all $a, b \in \{1, 2, 3, \ldots, n\}$: $(a\ b) \in \langle (1\ 2), (1\ 2\ 3\ 4 \ldots\ n) \rangle$.

   For (a) we use induction. The base case is $(1\ 2) \in \langle (1\ 2), (1\ 2\ 3 \ldots\ n) \rangle$. If we suppose that $(k\ k+1) \in \langle (1\ 2), (1\ 2\ 3\ 4 \ldots\ n) \rangle$, then we have

   $$(1\ 2\ 3\ 4 \ldots\ n)(k\ k+1)(1\ 2\ 3\ 4 \ldots\ n)^{-1} = (k+1\ k+2).$$

   For (b) we use induction. The base case is $(1\ 2) \in \langle (1\ 2), (1\ 2\ 3 \ldots\ n) \rangle$. If we suppose that $(1\ k) \in \langle (1\ 2), (1\ 2\ 3\ 4 \ldots\ n) \rangle$, then we have

   $$(k\ k+1)(1\ k)(k\ k+1)^{-1} = (1\ k+1).$$

   For (c) we notice that $(1\ a)(1\ b)(1\ a) = (a\ b)$.
   Therefore, since every permutation is a product of cycles and every cycle is a product of transpositions, we have that S_n is generated by $(1\ 2)$ and $(1\ 2\ 3\ 4 \ldots\ n)$.

2. Let T be the set of 3-cycles, and let $n \geq 3$. Every 3-cycle is an even permutation, therefore it belongs to A_n, and $\langle T \rangle \subseteq A_n$. Conversely, an element of A_n is a product of an even number of transpositions. Let σ and τ be two transpositions; if σ and τ are disjoint (i.e. their supports are disjoint sets), then we have $\sigma = (a\ b)$, $\tau = (c\ d)$, with a, b, c, d pairwise distinct, and $\sigma\tau = (c\ a\ d)(a\ b\ c) \in \langle T \rangle$. Otherwise, if σ and τ are not disjoint, we have $\sigma = \tau$ and $\sigma\tau = 1$, or $\sigma = (a\ b)$, $\tau = (b\ c)$ and $\sigma\tau = (b\ c\ a) \in \langle T \rangle$. In any case $\sigma\tau \in \langle T \rangle$, therefore a product of an even number of transpositions belongs to $\langle T \rangle$, so that $A_n \leq \langle T \rangle$ and $A_n = \langle T \rangle$.

3. Suppose that G has no elements of order 2. Then for any $g \in G \setminus \{1\}$ we have $g \neq g^{-1}$. Thus, pairing each non-trivial element with its inverse, we get $|G| = 1 + 2n$ for some $n \in \mathbb{N}$, which is a contradiction.

4. Consider the matrices (our A is the opposite of the one given in the Problem Sheet):

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

By computing the powers of A

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we see that A has order 4. Similarly we compute

$$B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and so the order of B is 3. Finally we compute

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has infinite order, as for $k \geq 1$

$$(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

This cannot happen in an abelian group. If a and b are of finite order and commute, then the order of ab divides the least common multiple of $o(a)$ and $o(b)$ (prove it!).

5. (a) Let $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_n}{s_n}$ rational numbers ($r_i, s_i \in \mathbb{Z}$, $s_i \neq 0$). Each $\frac{r_i}{s_i}$ is of the form $k_i \cdot \frac{1}{s_1 s_2 \cdots s_n}$, where $k_i = r_i s_1 s_2 \cdots s_{i-1} s_{i+1} \cdots s_n$. Therefore,

$$\left\langle \frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_n}{s_n} \right\rangle \subseteq \left\langle \frac{1}{s_1 s_2 \cdots s_n} \right\rangle.$$

This proves every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. Therefore, if $\mathbb{Q}$ were finitely generated, then it would be cyclic, say

$$\mathbb{Q} = \left\langle \frac{1}{m} \right\rangle$$

for some integer m. But $\frac{1}{2m} \notin \langle \frac{1}{m} \rangle$, therefore $\mathbb{Q}$ cannot be finitely generated.

(b) Suppose on the contrary that the multiplicative group of non-zero rational numbers is finitely generated and let

$$r_i = \frac{a_i}{b_i}$$

be the generators for $i = 1, \ldots, n$, where a_i, b_i are integers.
Then every non-zero rational number r can be written as

$$r = r_1^{c_1} \cdots r_n^{c_n} = \frac{a_1^{c_1} \cdots a_n^{c_n}}{b_1^{c_1} \cdots b_n^{c_n}}$$

for some integers $c_1, \ldots c_n$. Let p be a prime number that does not divide $b_1 \cdots b_n$, and consider $r = \frac{1}{p}$. Then we have

$$\frac{1}{p} = \frac{m}{b_1^{c_1} \cdots b_n^{c_n}}$$

for some integer m. Then we have

$$pm = b_1^{c_1} \cdots b_n^{c_n}$$

and this implies that p divides $b_1 \cdots b_n$, which contradicts our choice of the prime number p.

(c) We use the following result, whose prove is left as an exercise.
If G is a group and H is a normal subgroup of G such that both H and the quotient group G/H are finitely generated, then G is also finitely generated.
The group $(\mathbb{Z}, +)$ is finitely generated, as it is cyclic. If $\mathbb{Q}/\mathbb{Z}$ were finitely generated, then $(\mathbb{Q}, +)$ would be finitely generated, which we just showed is not true.

(d) Let G be the group in the question. We show that every finitely generated subgroup of G is proper. Let $H \leq G$ be finitely generated by $a_1/2^{e_1}, \ldots, a_n/2^{e_n}$. Then the denominators of the elements of H are all powers of 2 of exponent at most $m = \max(e_1, \ldots e_n)$. Thus $1/2^{m+1} \notin H$ and H is proper.

6. Let G be a non-cyclic group of order 4. Then $x^2 = 1$ for all $x \in G$, which implies $(xy)(xy) = 1$ for all $x, y \in G$. Multiply on the right by yx to get $xy = yx$, so that $G = \langle x \rangle \langle y \rangle \cong C_2 \times C_2$.

7. G is isomorphic to a product of cyclic groups whose orders are powers of p, say $G \cong \prod_{i=1}^{r} C_{p^{n_i}}$, where $n = n_1 + \cdots + n_r$. We can write $m = m_1 + \cdots + m_r$, where $m_i \leq n_i$ for $i = 1, \ldots r$. It is enough to prove that each $C_{p^{n_i}}$ contains a subgroup of order p^{m_i}, because then the product of these subgroups is a subgroup of G of order p^m. Let then $\langle g \rangle \cong C_{p^n}$, and let $1 \leq m \leq n$. The element $g^{p^{n-m}}$ generates a (cyclic) subgroup of order p^m, as wanted.

8. By the primary decomposition of a finite abelian group, the number of isomorphism classes of abelian groups of order p^n is equal to the number of partitions of n. For n up to 5 this is as listed in the following table, and can be seen by listing all partitions.

n	isomorphism classes
1	1
2	2
3	3
4	5
5	7

For $n = 4$ we have

$$1+1+1+1$$
$$2+1+1$$
$$2+2$$
$$3+1$$
$$4$$

For $n = 5$

$$1+1+1+1+1$$
$$2+1+1+1$$
$$2+2+1$$
$$3+2$$
$$4+1$$
$$5$$

9. We first work out the conjugacy classes of A_5 and their orders. The representatives of the cycle types of even permutations can be taken to be

$$1, \quad (1\ 2\ 3), \quad (1\ 2\ 3\ 4\ 5) \quad \text{and} \quad (1\ 2)(3\ 4).$$

Recall that the number of conjugates of an element s of a group G is the index $|G : C_G(s)|$ of the centraliser $C_G(s)$. The centralisers of 3-cycles and 5-cycles are as follows:

$$C_{A_5}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle \quad \text{and} \quad C_{A_5}((1\ 2\ 3\ 4\ 5)) = \langle (1\ 2\ 3\ 4\ 5) \rangle .$$

These groups have orders 3 and 5 (index 20 and 12), respectively, so there are 20 distinct conjugates of $(1\ 2\ 3)$ and 12 distinct conjugates of $(1\ 2\ 3\ 4\ 5)$ in A_5. Since there are a total of twenty 3-cycles in S_5 and all of these lie in A_5, we see that **all twenty 3-cycles are conjugate in A_5.**

There are a total of twenty-four 5-cycles in A_5 but only 12 distinct conjugates of the 5-cycle $(1\ 2\ 3\ 4\ 5)$. Thus some 5-cycle σ in *not* conjugate to $(1\ 2\ 3\ 4\ 5)$ in A_5, and we see that σ also has 12 distinct conjugates in A_5, hence **the 5-cycles lie in two conjugacy classes in A_5, each of which has 12 elements.**

Since the 3-cycles and the 5-cycles account for all non-identity elements of odd order, the 15 remaining non-identity elements of A_5 must have order 2 and therefore are double transpositions. It is easy to see that $(1\ 2)(3\ 4)$ commutes with $(1\ 3)(2\ 4)$ but does not commute with any non-identity element of odd order in A_5. It follows that $|C_{A_5}((1\ 2)(3\ 4))| = 4$. Thus $(1\ 2)(3\ 4)$ has 15 distinct conjugates in A_5, hence **all 15 elements of order 2 in A_5 are conjugate to $(1\ 2)(3\ 4)$.**

In summary, the conjugacy classes of A_5 have orders 1, 15, 20, 12 and 12. Now, suppose H were a normal subgroup of A_5. Then H would be a union of conjugacy classes of A_5. Then the order of H would be both a divisor of 60 (the order of A_5) and the sum of some collection of the integers $\{1, 12, 12, 15, 20\}$ (the sizes of the conjugacy classes of A_5). A quick check shows that the only possibilities are $|H| = 1$ or $|H| = 60$, so that A_5 has no proper, non-trivial normal subgroups.