Group Theory, 2016

Exercise sheet 5 (solutions)

Exercise 1. (a) Notice first that the scalar multiplication is well defined as if $[m] = [n]$ then $m = n + rp$ for some $r \in \mathbb{Z}$ and thus $mg = (n + rp)g = ng + r(pg) = ng + r \cdot 0 = ng$ for all $g \in G$.

Let us then go through the vector space axioms. Firstly $(G, +)$ is an abelian group by assumptions. Turning to the scalar multiplication, we have $[1] \cdot x = 1x = x$ (where the latter identity follows from the definition of nx). Then

$$[r] \cdot ([s] \cdot x) = [r] \cdot sx = r(sx) = (rs)x = [rs] \cdot x,$$

$$([r] + [x]) \cdot x = [r + s] \cdot x = (r + s)x = rx + sx = [r] \cdot x + [s] \cdot x$$

and

$$[r] \cdot (x + y) = r(x + y) = rx + ry = [r] \cdot x + [r] \cdot y.$$

(b) Suppose first that H is a subgroup of the group G. Then $0 \in H$ and H is closed under addition and taking additive inversers. It follows then as well that G is closed under scalar multiplication as $[m] \cdot x = mx \in H$. Thus H is a subspace of G.

Conversely, suppose that H is a subspace of G. Then $0 \in H$ and H is closed under addition. As $-x = [-1] \cdot x$, we also have that H is closed under taking additive inverses. Thus H is a subgroup of the group G.

Exercise 2.(a) Consider any finite number r of rationals. As these are finitely many we can represent these as fractions having the same denominator $n \geq 1$. Suppose these are $m_1/n, \ldots, m_r/n$. Notice that

$$\mathbb{Z}(m_1/n) + \cdots + \mathbb{Z}(m_r/n) \leq \mathbb{Z}(1/n) \neq \mathbb{Q}$$

as for example $1/(n + 1)$ is not in $\mathbb{Z}(1/n)$ or $1/p \notin \mathbb{Z}(1/n)$, where p is any prime that doesn't divide n. Hence $\mathbb{Q}$ can't be finitely generated.

(b) Let r/s and n/m be two rationals where r, n are integers and n, m positive integers. If one of these is zero, say r/s then $1 \cdot (r/s) + 0 \cdot (n/m) = 0$. If neither of these are zero then $sn(r/s) - mr(n/m) = 0$.

Exercise 3. (a) We have $144 = 2^4 \cdot 3^2$. The possible partitions of 2^4 and 3^2 into factors in increasing order are:

$$(16),\ (2, 8),\ (4, 4),\ (2, 2, 4),\ (2, 2, 2, 2)$$

and

$$(9),\ (3, 3).$$

There are thus $5 \cdot 2 = 10$ abelian groups of order 144,

$$\begin{aligned}
&\mathbb{Z}_{16} \oplus \mathbb{Z}_9,\ \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9,\ \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9,\\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9,\ \mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,\\
&\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,\\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3.
\end{aligned}$$

The abelian groups of order up to 15 are $\{0\}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_5$, $\mathbb{Z}_{11}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_{13}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_7$, $\mathbb{Z}_3 \oplus \mathbb{Z}_5$.

(b) Write A and B as a direct sum of cyclic groups of prime power order. By the Fundamental Theorem, it suffices to show that the cyclic summands for A and B are the same up to order. In other words that we have the same number of cyclic summands of order q for any prime power q. Suppose A has $a(q)$ cyclic summands of order q and that B has $b(q)$ such summands. As $A \oplus A$ and $B \oplus B$ are isomorphic, they have the same number of cyclic summands of order q. That is $2a(q) = 2b(q)$. If follows that $a(q) = b(q)$.

Exercise 4. First suppose $o(x_1), \ldots, o(x_n)$ are pairwise coprime. Consider the element $x = x_1 + \cdots + x_n$ and let m be the order of this element in G. As

$$0 = m(x_1 + \cdots + x_n) = mx_1 + \cdots + mx_n,$$

it follows from Proposition 2.2 that $mx_1 = \cdots = mx_n = 0$. Therefore $o(x_i)|m$ for $i = 1, \ldots, n$. As $o(x_1), \ldots, o(x_n)$ are coprime, it follows then that their product $o(x_1) \cdots o(x_n) = |G|$ divides $m = o(x)$. By Lagrange $o(x)$ divides $|G|$ and thus $o(x) = |G|$ which implies that $G = \mathbb{Z}x$.

Now suppose that some two of the orders have a common prime divisor. Let m be the least common multiple of $o(x_1), o(x_2), \ldots, o(x_n)$, then $m < o(x_1) \cdots o(x_n) = |G|$. As $o(x_i)|m$ for all $i = 1, \ldots, n$ it follows that $mx_1 = mx_2 = \ldots = mx_n = 0$. Hence for any $a_1x_1 + \cdots + a_nx_n$ in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$, we have

$$m(a_1x_1 + \cdots + ax_n) = 0.$$

It follow that $o(y) \leq m < |G|$ for all $y \in \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$ and so the group has no element of order $|G|$. Thus it can't be cyclic.

Exercise 5. We argue by contradiction and suppose that F^* is not cyclic. Using the Fundamental Theorem for finite abelian groups we know that F^* is an internal direct product,

$$F^* = \langle x_1 \rangle \cdots \langle x_n \rangle,$$

with cyclic factors of prime power order. By Exercise 4, some two of these must have orders that are power of the same prime. Without loss of generality suppose $o(x_1) = p^r$ and $o(x_2) = p^s$. Let $y_1 = x_1^{p^{r-1}}$ and $y_2 = x_2^{p^{s-1}}$. Then $o(y_1) = o(y_2) = p$ and we get at least p^2 elements of order p, namely

$$y_1^r y_2^s, \quad 0 \leq r, s \leq p - 1.$$

But then we have got at least p^2 roots for the polynomial $x^p - 1$ in $F[x]$ and this is absurd as there are at most p roots. (If say $a_1, \ldots, a_p$ are any p of the roots, then $x^p - 1 = (x - a_1) \cdots (x - a_p)$. But then $a^p = 1$ iff $(a - a_1) \cdots (a - a_p) = 0$ iff a is one of $a_1, \ldots, a_p$).