Queen Mary University of London

MTH4104 Introduction to Algebra

Week 12 coursework **due 19 April 2022**

You are to write up a careful and professionally presented solution to the question below. This is to be submitted on QMPlus as a single PDF or JPEG file by 12:00 noon, Tuesday 19 April 2022.

Question to submit

(a) Write out the Cayley table for $\mathbb{Z}_7^\times$. [4 marks]

(b) List all the subgroups of $\mathbb{Z}_7^\times$, including the "obvious" or "trivial" ones. Explain how you generated your list and how you know it is complete. [6 marks]

Solution (a)

$\cdot$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[2]_7$	$[2]_7$	$[4]_7$	$[6]_7$	$[1]_7$	$[3]_7$	$[5]_7$
$[3]_7$	$[3]_7$	$[6]_7$	$[2]_7$	$[5]_7$	$[1]_7$	$[4]_7$
$[4]_7$	$[4]_7$	$[1]_7$	$[5]_7$	$[2]_7$	$[6]_7$	$[3]_7$
$[5]_7$	$[5]_7$	$[3]_7$	$[1]_7$	$[6]_7$	$[4]_7$	$[2]_7$
$[6]_7$	$[6]_7$	$[5]_7$	$[4]_7$	$[3]_7$	$[2]_7$	$[1]_7$

Commentary. Since I have left off the brackets in some of my Cayley tables in the lecture notes, I don't object if you do the same here.

(b) The list of subgroups is:

- $\{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$
- $\{[1]_7, [2]_7, [4]_7\}$
- $\{[1]_7, [6]_7\}$
- $\{[1]_7\}$

Explanation. Every subgroup must contain the identity element $[1]_7$. We organise our search by working through the other elements the subgroup might contain, using this fact: if a subgroup contains another element g, then by the multiplicative closure law, it must also contain $g^2, g^3, \ldots$.

Because

$$[3]_7^2 = [2]_7 \qquad [3]_7^3 = [6]_7 \qquad [3]_7^4 = [4]_7 \qquad [3]_7^5 = [5]_7$$
$$[5]_7^2 = [4]_7 \qquad [5]_7^3 = [6]_7 \qquad [5]_7^4 = [2]_7 \qquad [5]_7^5 = [3]_7,$$

any subgroup containing $[3]_7$ or $[5]_7$ must contain every element of $\mathbb{Z}_7^\times$, i.e. it must *be* $\mathbb{Z}_7^\times$, first on our list. So now all that's left is to list the subgroups that don't contain $[3]_7$ or $[5]_7$.

Because $[2]_7^2 = [4]_7$ and $[4]_7^2 = [2]_7$, any subgroup containing one of these elements contains both. $\{[1]_7, [2]_7, [4]_7\}$ is a subgroup on our list. The only remaining possibility for a set containing these is $\{[1]_7, [2]_7, [4]_7, [6]_7\}$, but that is not a subgroup because it's not closed: $[2]_7[6]_7 = [5]_7$ is not in it. So now we're done with subgroups containing $[2]_7$ or $[4]_7$ as well.

What's left is subsets of $\{[1]_7, [6]_7\}$ containing $[1]_7$. There are two such subsets, and both of them are subgroups on our list.