## From Armstrong's Groups and Symmetry:

- Exercises (Chapter 5, pages 24-25):
5.2, 5.5, 5.10, 5.12

Problem A. Recall that $\mathbb{Z}_{11}^{\times}$is the multiplicative group of all invertible residue classes modulo 11.
(a) Check that [2] is a generator for $\mathbb{Z}_{11}^{\times}$. Conclude that $\mathbb{Z}_{11}^{\times}$is a cyclic group.
(b) Find the order of each element of $\mathbb{Z}_{11}^{\times}$.
(c) The group $\mathbb{Z}_{11}^{\times}$has exactly two non-trivial subgroups. List their elements.

Problem B. Let $U_{12}$ be the multiplicative group of 12 th roots of unity. That is, all solutions $z \in \mathbb{C}$ to the equation $z^{12}=1$. We know $U_{12}=\langle\zeta\rangle$ where

$$
\zeta=\cos \left(\frac{2 \pi}{12}\right)+i \sin \left(\frac{2 \pi}{12}\right)
$$

(a) Find the order of the elements of $U_{12}$. Circle those $\zeta^{n}$ for which $U_{12}=\left\langle\zeta^{n}\right\rangle$ :

(b) The group $U_{12}$ has exactly four non-trivial subgroups. List the elements of each subgroup, and plot them as points in the complex plane $\mathbb{C}$.
(c) Describe all the inclusions $(\subset)$ among the subgroups you found in (b).

Problem C. Consider the additive group $\mathbb{Z}_{18}$ of all residue classes modulo 18.
(a) List all $x \in \mathbb{Z}$ in the range $0 \leq x<18$ for which $\mathbb{Z}_{18}=\langle[x]\rangle$.
(b) The group $\mathbb{Z}_{18}$ has exactly four non-trivial subgroups. List the elements of each subgroup, and find all inclusions among the subgroups.
(c) Which of the groups below are cyclic? Circle the cyclic ones (and explain).

$$
\mathbb{Z}_{18} \times \mathbb{Z}_{18} \quad \mathbb{Z}_{18} \times \mathbb{Z}_{19} \quad \mathbb{Z}_{18} \times U_{12} \quad \mathbb{Z}_{18} \times \mathbb{Z}_{11}^{\times}
$$

(Recall the definition of direct products in Problem D on Homework 3.)

Problem D. Let $\mathbb{Z}$ be the additive group of all integers. Recall that $N \mathbb{Z}$ is the subgroup consisting of all integer multiple of $N$. Given two $M, N \in \mathbb{Z}$ consider

$$
M \mathbb{Z}+N \mathbb{Z}=\{M x+N y: x, y \in \mathbb{Z}\}
$$

(a) Explain why $M \mathbb{Z}+N \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and prove that

$$
M \mathbb{Z}+N \mathbb{Z}=\operatorname{GCD}(M, N) \mathbb{Z}
$$

(b) Check that $M \mathbb{Z} \cap N \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and show that

$$
M \mathbb{Z} \cap N \mathbb{Z}=\operatorname{LCM}(M, N) \mathbb{Z}
$$

(c) Give an example showing that $M \mathbb{Z} \cup N \mathbb{Z}$ is not always a subgroup.

