Reading notes on Chapter 4: Cyclic Groups

This short chapter deals with the type of group structures (groups and subgroups within larger groups) than can be generated by a single group element.

Let g be an element of a group G. The subgroup (although it may be all of G) generated by g is the set of all elements of G of the form g^n where $n \in \mathbb{Z}$. The notation for this subgroup is $\langle g \rangle$, i.e.

$$\langle g \rangle = \{g^n \,:\, n \in \mathbb{Z}\}.$$

Such (sub)groups are referred to as cyclic (sub)groups.

The chapter introduces this concept, gives some examples, in particular focussing on on the multiplicative group of complex numbers and the roots of unity.

The most signinficant result in the chapter might be Theorem 4.10 which establishes that every subgroup of a cyclic group is in fact cyclic. This prove uses the concepts of integer division with remainder and the well orderedness of the integers, concepts familiar to you from your Number Theory studies last year. The theorems following 4.10 give further applications of these number theoretic concepts to cyclic groups.

Chapter 4 exercises

Section 4.4 contains a large number of useful exercises.

- Questions 1 through 22 focus mainly on examples. Many of these exercises concern the complex numbers and number theory type exercises which should be familiar to you.
- From question 23 on we find questions of a more abstract group-theoretic nature.

Sage exercises

Section 4.8 is a guided exploration of what Judson refers to as $U(n)$, the group of units (elements with multiplicative inverses) from the additive group $\mathbb{Z}_n$. This is the same as the group that we dealt with in Number Theory last year which we referred to as $\mathbb{Z}_n^{\times}$.