Exercise 1. For x an element of a group G, show that x and x^{-1} have the same order. 1.1.20

Solution. Suppose $|x| = n$. First of all, since $x^n = 1$, we have that $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$. Therefore, $|x^{-1}|$ is equal to n unless there is an $m < n$ such that $(x^{-1})^m = 1$. Suppose that such an m exists. Then $(x^{-1})^m = 1$, but since $(x^{-1})^m x^m = 1$ as well, this implies that $x^m = 1$, which is a contradiction.
If there is no finite n such that $|x| = n$ (i.e. $|x| = \infty$), then we must have $|x^{-1}| = \infty$. Indeed, if $|x^{-1}| = n$ for some finite n, then $|x| = n$ by the argument above, which is a contradiction.

Exercise 2. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. We can deduce that $|x| \leq |G|$. 1.1.32

Solution. Suppose that this is not the case, and there exists $1 \leq k < l \leq n-1$ such that $x^k = x^l$. (We know already that 1 is distinct from the others.) Then $x^k = x^l = x^{k+(l-k)} = x^k x^{l-k}$. However, this implies that $x^{l-k} = 1$, which contradicts $|x| = n$ since $1 \leq l-k \leq n-2$.

Exercise 3. Show that $\mathbb{Z}/n\mathbb{Z}$ is a group under addition of residue classes. You may notice a similarity to the cyclic group described in the previous section. These groups are isomorphic, which is a concept that we'll define formally later on in Chapter 1.

Solution. We start with showing that addition on residue classes is associative. Let $\overline{a}, \overline{b}, \overline{c}$ be three elements of $\mathbb{Z}/n\mathbb{Z}$. Then we have

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{a+b+c} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}),$$

by the assumption that addition of residue classes is well-defined and the fact that addition of integers is associative. Next, we check that we have an identity element. Consider $\overline{0}$. For any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, we have that $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$ (and similarly for $\overline{0} + \overline{a}$).
Finally, we check that we have inverses. For each $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, its inverse is $\overline{-a}$, since $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$ (and similarly for $\overline{-a} + \overline{a}$).

Exercise 4. Show that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative. Then, show that, for $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes. 1.1.4 1.1.5

Solution. Let $\overline{a}, \overline{b}, \overline{c}$ be three elements of $\mathbb{Z}/n\mathbb{Z}$. Then we have

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{a \cdot b \cdot c} = \overline{a} \cdot \overline{b \cdot c} = \overline{a} \cdot (\overline{b} \cdot \overline{c}),$$

by the assumption that multiplication of residue classes is well-defined and the fact that multiplication of integers is associative.
Consider $\mathbb{Z}/4\mathbb{Z}$. In this set, we have that $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$. This is a problem, since it implies that the element $\overline{2}$ does not have an inverse. There is no element $\overline{2}^{-1}$ such that $(\overline{2} \cdot \overline{2}) \cdot \overline{2}^{-1} = \overline{2} \cdot (\overline{2} \cdot \overline{2}^{-1}) = \overline{2}$.

Exercise 5. Find the orders of each element of the additive group $\mathbb{Z}/8\mathbb{Z}$. 1.1.11

Solution. Trivially, we have $|\overline{0}| = 1$. Then, for example, for $\overline{2}$, we check that $\overline{2} = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{6}$, $\overline{2}^4 = \overline{8} = \overline{0}$. Therefore, $|\overline{2}| = 4$. Similarly, we find the orders of all elements of this group:

$$\begin{array}{ll} |\overline{0}| = 1 & |\overline{4}| = 2 \\ |\overline{1}| = 8 & |\overline{5}| = 8 \\ |\overline{2}| = 4 & |\overline{6}| = 4 \\ |\overline{3}| = 8 & |\overline{7}| = 8. \end{array}$$

Of course, there is an easier way to find these than brute force. Do you see the pattern?

Exercise 6. Use generators and relations to show that if x is any element of D_{2n}, which is not a power of r, then $rx = xr^{-1}$. 1.2.2

Solution. We have seen that we can write any element of D_{2n} in the form $s^i r^j$, where $0 \leq i \leq 1$ and $0 \leq j \leq n-1$. Since x is not a power of r we have $x = sr^j$. Then

$$rx = rsr^j = sr^{-1}r^j = sr^{j-1} = sr^j r^{-1} = xr^{-1}.$$