

1 Homework 1: your basic toolkit

Remember:

- Homework is due on the 10th of September before class.
- Please cite any source/collaboration.
- You do not have to hand it your homework in LaTeX till the 5th Monday but you are encouraged to start early!

Exercise 1.1. Prove the fundamental theorem of arithmetic. You might have to resort to other sources, but please express your solution in your own words. The point of this exercise is to acquaint you with proof techniques. Here's the statement

Theorem 1.2. *Let n be an integer > 1 . Then n can be written as*

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$$

where p_i 's are distinct primes and $\alpha_i \geq 0$. This expression is unique up to rearrangement of the factors.

Exercise 1.3. The integers form the collection

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$$

Here are the rules of arithmetic in \mathbb{Z} :

1. If $a, b \in \mathbb{Z}$ then $a + b \in \mathbb{Z}$.

2. If $a, b \in \mathbb{Z}$ then $a \cdot b \in \mathbb{Z}$.

3. If $a, b, c \in \mathbb{Z}$ then

$$(a + b) + c = a + (b + c).$$

4. If $a, b, c \in \mathbb{Z}$ then

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

5. If $a, b \in \mathbb{Z}$ then

$$a \cdot b = b \cdot a.$$

6. There exists $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$

$$a + 0 = 0 + a = a.$$

Such an element is called a **additive identity**.

7. There exists $1 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$

$$a \cdot 1 = 1 \cdot a = a$$

Such an element is called a **multiplicative identity**.

8. For all $a \in \mathbb{Z}$ there exists $-a$ such that

$$a + (-a) = 0 = (-a) + a$$

Such an element is called an **additive inverse**.

Prove, using the rules of arithmetic in \mathbb{Z} :

1. Additive and multiplicative identities are unique.
2. Additive inverses are unique.
3. If $a, b, c \in \mathbb{Z}$ and $a + b = a + c$ then $b = c$.
4. If $a \in \mathbb{Z}$ then $(-1) \cdot a = -a$.
5. If $a, b \in \mathbb{Z}$ then $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
6. If $a, b \in \mathbb{Z}$ then $(-a) \cdot (-b) = ab$.

Exercise 1.4. A **permutation on n -letters** is a way of rearranging the set $\underline{n} := \{1, \dots, n\}$. So for example we can rearrange $\{1, 2, 3\}$ as $\{1, 3, 2\}$. Prove that the number of permutation on n -letters is exactly $n!$.

Exercise 1.5. Let X be a set with n elements. Prove that X has 2^n subsets.

Exercise 1.6. Suppose that $n \geq 4$. Prove by induction that $n! > 2^n$.

Exercise 1.7. Let X be a set and \sim be an equivalence relation. Define $C(a) := \{b \in X : b \sim a\}$. Prove

1. $a \in C(a)$.
2. If $a \sim b$ then $C(a) = C(b)$.
3. If a is not $\sim b$ then $C(a) \cap C(b) = \emptyset$.
4. $\bigcup_{a \in X} C(a) = X$.

Illustrate, by means of a picture, what an equivalence relation looks like in light of the above result.

Exercise 1.8. Let A, B, C be sets. Prove

1. $A \subseteq A$.
2. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
3. If $A \subseteq B, B \subseteq C$ then $A \subseteq C$.
4. $\emptyset \subseteq A$ always.
5. $A \cup (B \cap C) = (A \cup B) \cap C$
6. $A \cap (B \cup C) = (A \cap B) \cup C$
7. $A \cup \emptyset = A$
8. $A \cup B = \emptyset$ if and only if $A = \emptyset$ and $B = \emptyset$
9. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
10. $(A \cup B)^c = A^c \cap B^c$
11. $(A \cap B)^c = A^c \cup B^c$.

Exercise 1.9. Prove that if A has m elements, B has n elements, then $A \times B$ has mn elements.

2 Homework 2: Sets and fields

Exercise 2.1. Let p be a prime. Prove that for all $x \in \mathbb{Z}/p$ there exists a $y \in \mathbb{Z}/p$ such that $x \cdot y = 1$. Furthermore, such a y is unique.

References