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*

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

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

Exercise 1.3. The integers form the collection

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

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 $\underline{n} := \{1, \cdots, n\}$. 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 $n \geqslant 4$. 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. $A \cup (B \cup C) = (A \cup B) \cup C$
6. $A \cap (B \cap C) = (A \cap B) \cap C$
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. Write down explicitly the addition and multiplication table for $\mathbb{Z}/3$.

Exercise 2.2. Prove that multiplication in $\mathbb{Z}/n$ is well-defined.

Exercise 2.3. True or false: on the set with one element, there is a unique field structure. Justify your answer

Exercise 2.4. Let k be an field. Prove:

1. for any nonzero element $x \in k$ there exists a unique y such that $xy = 1$. We denote this by x^{-1}
2. For any nonzero element $x \in k$, $(x^{-1})^{-1} = x$.

Exercise 2.5. Let k be a field. Consider the set $k \times k$ endowed with the "pointwise" multiplication and addition: $(x, y) + (x', y') = (x + x', y + y')$ and $(x, y) \cdot (x', y') = (x \cdot x', y \cdot y')$ and the additive identity being $(0, 0)$ and the multiplicative one being $(1, 1)$. True or false: this endows $k \times k$ with the structure of a field. Justify your answer.

Exercise 2.6. Let k be a field and $x, y, z \in k$. Then $x = y$ if and only if $x + z = y + z$.

Exercise 2.7. Let p be a prime. Prove that the following equation holds in $\mathbb{F}_p$:

$$(x + y)^p = x^p + y^p.$$

Exercise 2.8. Let $f : X \to Y, g : Y \to Z$ be functions. Prove that

1. if f, g are injective then $g \circ f$ is injective.
2. if $g \circ f$ is injective then f is injective.
3. True or false: if $g \circ f$ is injective then g is injective. Prove or give a counterexample.

Exercise 2.9. Let $f : X \to Y, g : Y \to Z$ be functions. Prove that

1. if f, g are surjective then $g \circ f$ is surjective.
2. if $g \circ f$ is surjective then g is surjective.
3. True or fase: if $g \circ f$ is surjective then f is surjective. Prove or give a counterexample.

3 Homework 3: Vector spaces and their subspaces

Exercise 3.1. Let k be a field and S be a set. Then let k^S denote the set of functions

$$f : S \to k.$$

For $f, g \in k^S$, define addition $f+g$ to be the function that sends $s \in S$ to $f(s)+g(s)$, i.e. $(f+g)(s) = f(s)+g(s)$. For $a \in k$ and $f \in k^S$, define scalar multiplication af to be the function that sends $s \in S$ to $af(s)$, i.e. $(af)(s) = af(s)$.

1. Prove that with this addition and scalar multiplication, k^S is a vector space over k.
2. What is the additive inverse $-f$ of a function $f \in k^S$?

Exercise 3.2. Which of the following is *not* a vector space over $\mathbb{R}$? If it is not, explain why.

1. $\mathbb{R}$ itself, with its ordinary addition and scalar multiplication.
2. $\mathbb{C}$ with ordinary addition and scalar multiplication.
3. The set $\{0\}$, with the only possible addition and scalar multiplication.
4. The empty set $\varnothing$ (which has no elements).
5. The set $\mathbb{R} \cup \{\infty, -\infty\}$ with elements given by the real numbers together with two additional elements ∞ and $-\infty$. The addition and scalar multiplication is as usual on the subset of $\mathbb{R}$ of $\mathbb{R} \cup \{\infty, -\infty\}$. We extend addition to all elements of $(\mathbb{R} \cup \{\infty, -\infty\}) \times (\mathbb{R} \cup \{\infty, -\infty\})$ by

$$\begin{aligned} x + \infty = \infty &= \infty + x && \text{for all } x \in \mathbb{R} \\ x + (-\infty) = -\infty &= (-\infty) + x && \text{for all } x \in \mathbb{R} \\ \infty + \infty &= \infty \\ (-\infty) + (-\infty) &= -\infty \\ \infty + (-\infty) = 0 &= (-\infty) + \infty, \end{aligned}$$

and extend scalar multiplication to all elements of $\mathbb{R} \times (\mathbb{R} \cup \{\infty, -\infty\})$ by

$$a\infty = \begin{cases} \infty & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -\infty & \text{if } a < 0, \end{cases} \qquad a(-\infty) = \begin{cases} -\infty & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ \infty & \text{if } a < 0. \end{cases}$$

References