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, subspaces and spans

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

$$f \colon S \to k.$$

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

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

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

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

Exercise 3.3. Let V be a k-vector space. Suppose that 0_k is the additive identity in the field and 0_V is the additive identity of the vector space. Then prove:

1. The additive identity 0_V of V is unique.
2. $0_k v = 0_V$ for all $v \in V$
3. $\alpha 0_V = 0_V$ for all $\alpha \in k$
4. $(-1)v = -v$ for all $v \in V$.

Exercise 3.4. Let k be a field and V a vector space. Consider the function

$$\alpha\cdot : V \to V \qquad v \mapsto \alpha \cdot v.$$

Is the function

1. injective?
2. surjective?
3. bijective?

Prove or give a counterexample.

Exercise 3.5. Consider the vector space from Question 3.1, which we denote by k^S. Consider the subset

$$k^S_{\text{fin}} := \{f : S \to k : \text{for all but finitely many } s \in S,\ f(s) = 0\}.$$

Prove or disprove: k^S_{fin} is a subspace of k^S.

Exercise 3.6. Let k be a field and consider

$$\text{Poly}_k := \{p(x) = a_n x^n + a_{n-1}x^n - 1 + \cdots + a_0 : a_i \in k\},$$

the set of polynomials over k. Take for granted that Poly_k is a vector space over k. Let $m \geqslant 0$. True or false: the subset

$$\text{Poly}_{k,\leqslant m} := \{p(x) = a_n x^n + a_{n-1}x^n - 1 + \cdots + a_0 : a_i \in k, n \leqslant m\}$$

is a subspace of Poly_k.

Exercise 3.7. Let V be a vector space and let U_1, U_2 be subspaces of V. Prove that

1. $U_1 \cap U_2$ is a subspace of V.
2. Define $U_1 + U_2 := \{u_1 + u_2 : u_1 \in U_1, u_2 \in U_2\}$; this is a subspace of V.

Is the union $U_1 \cup U_2$ a subspace of V?

Exercise 3.8. Let k be a field with finitely many elements. Prove that

1. Prove that a vector space V over k is finite-dimensional if and only if it has finitely many elements.
2. Prove that if V is a finite-dimensional vector space over k, it has $(\#k)^{\dim(V)}$ elements.

Exercise 3.9. Which of the vector spaces (and subspaces) above are finite dimensional? (No need to give detailed proof)

4 Homework 4: linear transformations

Exercise 4.1. Let V, W be vector spaces over a field k and $f : V \to W$ a linear transformation. Then prove that $f(0) = 0$ and $f(-v) = -f(v)$.

Exercise 4.2. Suppose that $f : V \to W, g : W \to U$ be linear maps, then prove that

1. $g \circ f : V \to U$ is a linear map,
2. If $h : W \to U$ is another linear map prove that $(h + g) \circ f = h \circ f + h \circ g$,
3. if $i : V \to W$ is another linear map prove that $g \circ (f + i) = g \circ f + g \circ i$.

Exercise 4.3. Let $f : V \to W$ be an injective linear transformation. Suppose that $\{v_1, \cdots, v_n\}$ is a linearly independent list of vectors, prove that $\{f(v_1), \cdots, f(v_n)\}$ is linearly independent.

Exercise 4.4. Let k be a field, consider the function

$$\sigma_n : k^{\times n} \to k^{\times n} \qquad (x_1, \cdots, x_n) \mapsto (x_n, x_1, \cdots, x_{n-1})$$

Prove that this a linear transformation and write down the corresponding matrix.

Exercise 4.5. Prove that the only linear transformations from a 1-dimensional vector space to itself is given by scalar multiplication.

Exercise 4.6. Let $D : \mathrm{Poly}_{\leqslant d}(k) \to \mathrm{Poly}_{\leqslant d-1}(k)$ be "differentiation" as a linear map. Prove that D^{d+1} is the zero transformation.

Exercise 4.7. Let $g, f : V \to V$ be a linear transformation and suppose that $\dim V = n$. Prove that

1. $\dim(\mathrm{Im}(f \circ g)) \leqslant \min\{\dim(\mathrm{Im}(f)), \dim(\mathrm{Im}(g))\}$.
2. $\dim(\mathrm{Im}(f)) + \dim(\mathrm{Im}(g)) \leqslant \dim(\mathrm{Im}(f \circ g)) + n$.

5 Homework 5: rank-nullity, duals

Exercise 5.1. Suppose that V, W are vector spaces over a field k. Then $\dim(V) = \dim(W)$ if and only if V is isomorphic to W (hint: please construct the linear map $f : V \to W$ or $g : W \to V$).

Exercise 5.2. Suppose that $W_0 \xrightarrow{f} W_2 \xleftarrow{g} W_1$ are linear maps. Consider the vector space

$$W_0 \times_{W_2} W_1 := \{(w_0, w_1) : f(w_0) = g(w_1)\}.$$

Prove that

1. under pointwise addition and scalar multiplication, $W_0 \times_{W_2} W_1$ is a vector space.
2. Prove that the kernel of the map

   $$W_0 \times_{W_2} W_1 \to W_0 \qquad (w_0, w_1) \mapsto w_0$$

   is isomorphic to the kernel of the map $W_1 \to W_2$.
3. Assume that $W_1 \to W_2$ is surjective. Compute the dimension of $W_0 \times_{W_2} W_1$.

Exercise 5.3. Consider an exact sequence of finite dimensional vector spaces $0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$ (this means that $0 \to V_1 \to V_2$ is exact for all i $V_i \to V_{i+1} \to V_{i+2}$ is exact and $V_{n-1} \to V_n \to 0$ is exact). Prove that

$$\sum_{i=0}^{n} (-1)^i \dim V_i = 0.$$

Exercise 5.4. Prove that if $U_1, \cdots U_n$ are subspaces of V, then $U_1 + U_2 + \cdots + U_n$ is isomorphic to $U_1 \oplus U_2 \oplus \cdots U_n$ if and only if $\dim(U_1 + \cdots + U_n) = \dim(U_1) + \dim(U_2) + \cdots + \dim(U_n)$.

Exercise 5.5. Suppose that $0 \to V' \to V \to V'' \to 0$ is an exact sequence of vector spaces, then V is isomorphic to $V'' \oplus V'$.

Exercise 5.6. Suppose that $V' \to V \to V''$ is an exact sequence of vector spaces, then prove that taking duals preserves exactness, i.e., the following is an exact sequence

$$(V')^\vee \to V^\vee \to (V'')^\vee.$$

Exercise 5.7. Let V be a finite dimensional vector space. Define a map

$$T : V \to (V^\vee)^\vee,$$

by sending v to the linear functional on the dual given by

$$(Tv)(\phi) = \phi(v).$$

Prove that this map is linear and that it is an isomorphism.

Exercise 5.8. Consider $\mathrm{Poly}_{\leqslant 2}(k)$ as a vector space and consider the subspace spanned by x^2, which we call U. Consider the function

$$\phi : \mathrm{Poly}_{\leqslant 2}(k) \to k \qquad \phi(p) = p'(0).$$

1. prove that ϕ is a linear functional.
2. Show that $\mathrm{Span}(\phi) \subset \mathrm{Ann}(U)$; show that the inclusion is proper and complete explicitly to a basis of $\mathrm{Ann}(U)$.

Exercise 5.9. Consider $\mathrm{Poly}_{\leqslant d}(k)$ and suppose that $x \in k$ is a non-zero element. Prove that $1, x-k, (x-k)^2, \cdots, (x-k)^d$ is a basis. Write down the dual basis, i.e., define linear functions $\phi_i : \mathrm{Poly}_{\leqslant d}(k) \to k$ which is dual to the above basis.

6 Homework 6: duals and transposes, a little eigenstuff

Exercise 6.1. Consider $D : \mathrm{Poly}_{\leqslant d}(k) \to \mathrm{Poly}_{\leqslant d-1}(k)$ be "differentiation" as a linear map. Write down D as a matrix and write down its transpose.

Exercise 6.2. Let k be a field, consider the linear map

$$\sigma_n : k^{\times n} \to k^{\times n} \qquad (x_1, \cdots, x_n) \mapsto (x_n, x_1, \cdots, x_{n-1})$$

Write down its transpose matrix.

Exercise 6.3. Let $f : V \to W$ be a linear map between finite dimensional vector spaces. Prove that $\mathrm{Im}(f^\vee) \subset \mathrm{Ann}(\ker(f))$.

Exercise 6.4. Suppose that $f : V \to V$ is an isomorphism with inverse g. Prove that $f^\vee$ is an isomorphism as well and that the inverse of $f^\vee$ is given by $g^\vee$. Conclude that if A is an $n \times n$-matrix with transpose A^t then $(A^{-1})^t = (A^t)^{-1}$.

Exercise 6.5. Let V be a finite dimensional vector space and $U, W \subset V$ are subspaces. Prove that $\mathrm{Ann}(U \cap W) = \mathrm{Ann}(U) + \mathrm{Ann}(W)$.

Exercise 6.6. Let V be n-dimensional and suppose that a linear map $f\colon V \to V$ satisfies $f^2 = f$ (then it is called an *idempotent*).

1. Prove that the identity and the 0 maps are idempotent.
2. Produce an idempotent on $k^{\times 2}$ which is not the identity or the zero map.
3. Prove that $(\mathrm{id} - f)^2 = \mathrm{id} - f$.
4. Prove that $\dim \mathrm{im}(\mathrm{id} - f) = \dim \ker(f)$ and $\dim \mathrm{im}(f) = \dim \ker(\mathrm{id} - f)$.
5. Prove that $V = \mathrm{im}(f) \oplus \mathrm{im}(\mathrm{id} - f)$.
6. Prove that only $0, 1$ can be eigenvalues of f.

7 Homework 7: eigenstuff

Recall that the determinant of a 2×2 matrix:

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is given by $\det(M) = ad - bc$ while the trace is given by $\mathrm{tr}(A) = a + d$

Exercise 7.1. Let M be a 2×2 matrix. Prove that the eigenvalues of M are given by the roots of the polynomial

$$x^2 - \mathrm{tr}(M)x + \det(M)$$

Exercise 7.2. Define numbers by setting $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 3$. The sequence $\{F_n\}$ is known as *Fibonacci's sequence*.

1. Define a linear map $f : \mathbb{R}^2 \to \mathbb{R}^2$ by $f(x, y) = (y, x + y)$. Prove that $f^n(0, 1) = (F_n, F_{n+1})$; here f^n indicates the composition of f with itself n-times.
2. Find the eigenvalues and corresponding eigenvectors of f.
3. Use this to prove that
$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right].$$

Exercise 7.3. A matrix is called *nilpotent* if $A^n = 0$ for some $n \geqslant 0$. Prove that if A is a nilpotent matrix then $(1 - A)$ is invertible (Hint: if x is an indeterminate then it is always true that

$$\frac{1}{1 - x} = 1 + x + x^2 + \cdots x^n + \cdots .$$

)

Exercise 7.4. Let A be a matrix with a nonzero eigenvalue λ. Show that there is a vector v such that $A^k v = 0$ for all $k \geqslant 0$. Prove that every nilpotent matrix must have eigenvalue zero.

Exercise 7.5. Consider a linear map

$$f : k^{\times n} \to k^{\times n} : (x_1, \cdots, x_n) \mapsto (x_1 + x_2, x_2 + x_3, \cdots, x_{n-1} + x_n, x_n).$$

Prove that the matrix of f in the standard basis is upper triangular. What are its eigenvalues? Is it diagonalizable?

Exercise 7.6. True or false. Justify your answers.

1. Consider the linear map $k^{\times 2} \to k^{\times 2}, (x, y) \mapsto (y, x)$. Then its matrix is diagonalizable over the real numbers.
2. Consider the linear map $k^{\times 2} \to k^{\times 2}, (x, y) \mapsto (-y, x)$. Then its matrix is diagonalizable over the real numbers.
3. Consider the linear map $k^{\times 2} \to k^{\times 2}, (x, y) \mapsto (-y, x)$. Then its matrix is diagonalizable over the complex numbers.

4. Consider the matrix
$$M = \begin{bmatrix} 1 & x \\ c & 1 \end{bmatrix}$$
Then if k is a field of characteristic p, $M^p = \mathrm{id}$.

5. Consider the situation of the previous question. Then M is diagonalizable (Hint: use the first problem to determine the eigenvalues of M).

Exercise 7.7. Let $f : V \to V$ be a linear map. Prove that the generalized eigenspace of λ is equal to the kernel of the linear map $(f - \mathrm{id})^{\dim V}$.

References