Lior Silberman’s Math 412: Problem Set 1 (due 12/9/2019)

Practice problems, any sub-parts marked “OPT” (optional) and supplementary problems are not for submission.

Practice problems

P1 Show that the map $f: \mathbb{R}^3 \to \mathbb{R}$ given by $f(x,y,z) = x - 2y + z$ is a linear map. Show that the maps $(x,y,z) \mapsto 1$ and $(x,y,z) \mapsto x^2$ are non-linear.

P2 Let $F$ be a field, $X$ a set. Carefully show that pointwise addition and scalar multiplication endow the set $F^X$ of functions from $X$ to $F$ with the structure of an $F$-vectorspace.

For submission

RMK This problem introduces a device for showing that sets of vectors are linearly independent. Make sure you understand how this argument works by solving 1(d), 2(a), 1(e).

1. Let $V$ be a vector space, $S \subset V$ a set of vectors. A minimal dependence in $S$ is an equality
   \[ \sum_{i=1}^{m} a_i v_i = 0 \]
   where $v_i \in S$ are distinct, $a_i$ are scalars not all of which are zero, and $m \geq 1$ is as small as possible so that such $\{a_i\}$, $\{v_i\}$ exist.

   — It is implicit in the following that either $S$ is independent or it has a minimal dependence. Make this explicit in your mind (don’t write this bit up).

   (a) Find a minimal dependence among
   \[ \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 2 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^3. \]

   (b) Show that in a minimal dependence the $a_i$ are all non-zero.

   (c) Suppose that $\sum_{i=1}^{m} a_i v_i$ and $\sum_{i=1}^{m} b_i v_i$ are minimal dependences in $S$, involving the exact same set of vectors. Show that there is a non-zero scalar $c$ such that $a_i = cb_i$.

   (d) Let $T: V \to V$ be a linear map, and let $S \subset V$ be a set of (non-zero) eigenvectors of $T$, each corresponding to a distinct eigenvalue. Applying $T$ to a minimal dependence in $S$ obtain a contradiction to (c) and conclude that $S$ is actually linearly independent.

   (*e) Let $\Gamma$ be a group. The set $\text{Hom}(\Gamma, \mathbb{C}^\times)$ of group homomorphisms from $\Gamma$ to the multiplicative group of nonzero complex numbers is called the set of quasicharacters of $\Gamma$ (the notion of “character of a group” has an additional, different but related meaning, which is not at issue in this problem). Show that $\text{Hom}(\Gamma, \mathbb{C}^\times)$ is linearly independent in the space $\mathbb{C}^\Gamma$ of functions from $\Gamma$ to $\mathbb{C}$.

2. Let $S = \{ \cos(nx) \}_{n=0}^{\infty} \cup \{ \sin(nx) \}_{n=1}^{\infty}$, thought of as a subset of the space $C(\mathbb{R}, \mathbb{C})$ of continuous functions on the interval $[-\pi, \pi]$.

   (a) Applying $\frac{d}{dx}$ to a putative minimal dependence in $S$ obtain a different linear dependence of at most the same length, and use that to show that $S$ is, in fact, linearly independent.

   (b) Show that the elements of $S$ are an orthogonal system with respect to the inner product $\langle f, g \rangle = \int_{-\pi}^{\pi} f(x)g(x) \, dx$ (feel free to look up any trig identities you need). This gives a different proof of their independence.

   (c) Let $W = \text{Span}_C(S)$ (this is usually called “the space of trigonometric polynomials”; a typical element is $5 - \sin(3x) + \sqrt{2}\cos(15x) - \pi\cos(32x)$). Find a ordering of $S$ so that the matrix of the linear map $\frac{d}{dx}: W \to W$ in that basis has a simple form.
3. (Matrices associated to linear maps) Let $V, W$ be vector spaces of dimensions $n, m$ respectively. Let $T \in \text{Hom}(V, W)$ be a linear map from $V$ to $W$. Show that there are ordered bases $B = \{v_j\}_{j=1}^n \subset V$ and $C = \{w_j\}_{i=1}^m \subset W$ and an integer $d \leq \min\{n, m\}$ such that the matrix $A = (a_{ij})$ of $T$ with respect to those bases satisfies $a_{ij} = \begin{cases} 1 & i = j \leq d \\ 0 & \text{otherwise} \end{cases}$, that is has the form

$$
\begin{pmatrix}
1 & & & & \\
& \ddots & & & \\
& & 1 & & \\
& & & \ddots & \\
& & & & 0
\end{pmatrix}
$$

(Hint1: study some examples, such as the matrices $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}$) (Hint2: start your solution by choosing a basis for the image of $T$).

**Extra credit: Finite fields**

4. Let $F$ be a field.
   (a) Define a map $t: (\mathbb{Z}, +) \to (F, +)$ by mapping $n \in \mathbb{Z}_{\geq 0}$ to the sum $1_F + \cdots + 1_F$ $n$ times. Show that this is a group homomorphism.
   
   DEF If the map $t$ is injective we say that $F$ is of **characteristic zero**.
   
   (b) Suppose there is a non-zero $n \in \mathbb{Z}$ in the kernel of $t$. Show that the smallest positive such number is a prime number $p$.
   
   DEF In that case we say that $F$ is of **characteristic $p$**.
   
   (c) Show that in that case $t$ induces an isomorphism between the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and a subfield of $F$. In particular, there is a unique field of $p$ elements up to isomorphism.

5. Let $F$ be a field with finitely many elements.
   (a) Carefully endow $F$ with the structure of a vector space over $\mathbb{F}_p$ for an appropriately chosen $p$.
   
   (b) Show that there exists an integer $r \geq 1$ such that $F$ has $p^r$ elements.
   
   RMK For every prime power $q = p^r$ there is a field $\mathbb{F}_q$ with $q$ elements, and two such fields are isomorphic. They are usually called **finite fields**, but also **Galois fields** after their discoverer.

**Supplementary Problems I: A new field**

A. Let $\mathbb{Q}(\sqrt{2})$ denote the set $\left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\} \subset \mathbb{R}$.
   
   (a) Show that $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-subspace of $\mathbb{R}$.
   
   (b) Show that $\mathbb{Q}(\sqrt{2})$ is two-dimensional as a $\mathbb{Q}$-vector space. In fact, identify a basis.
   
   (*c) Show that $\mathbb{Q}(\sqrt{2})$ is a field.
   
   (**d) Let $V$ be a vector space over $\mathbb{Q}(\sqrt{2})$ and suppose that $\dim_{\mathbb{Q}(\sqrt{2})} V = d$. Show that $\dim_{\mathbb{Q}} V = 2d$. 

9
Fix a field $F$.

B. (The general linear group)

(a) Let $\text{GL}_{n}(F)$ denote the set of invertible $n \times n$ matrices with coefficients in $F$. Show that $\text{GL}_{n}(F)$ forms a group with the operation of matrix multiplication.

(b) For a vector space $V$ over $F$ let $\text{GL}(V)$ denote the set of invertible linear maps from $V$ to itself. Show that $\text{GL}(V)$ forms a group with the operation of composition.

(c) Suppose that $\dim_{F} V = n$ Show that $\text{GL}_{n}(F) \cong \text{GL}(V)$ (hint: show that each of the two group is isomorphic to $\text{GL}(F^{n})$).

C. (Group actions) Let $G$ be a group, $X$ a set. An action of $G$ on $X$ is a map $\cdot : G \times X \to X$ such that $g \cdot (h \cdot x) = (gh) \cdot x$ and $1_{G} \cdot x = x$ for all $g, h \in G$ and $x \in X$ ($1_{G}$ is the identity element of $G$).

(a) Show that matrix-vector multiplication $(g, v) \mapsto gv$ defines an action of $G = \text{GL}_{n}(F)$ on $X = F^{n}$.

(b) Let $V$ be an $n$-dimensional vector space over $F$, and let $B$ be the set of ordered bases of $V$.

For $g \in \text{GL}_{n}(F)$ and $B = \{v_{i}\}_{i=1}^{\dim V} \in B$ set $gB = \left\{ \sum_{j=1}^{n} g_{ij}v_{j} \right\}_{j=1}^{n}$. Check that $gB \in B$ and that $(gB) \mapsto gB$ is an action of $\text{GL}_{n}(F)$ on $B$.

(c) Show that the action is transitive: for any $B, B' \in B$ there is $g \in \text{GL}_{n}(F)$ such that $gB = B'$. (d) Show that the action is simply transitive: that the $g$ from part (b) is unique.

D. (From the physics department) Let $V$ be an $n$-dimensional vector space, and let $B$ be its set of bases. Given $u \in V$ define a map $\phi_{u} : B \to F^{n}$ by setting $\phi_{u}(B) = a$ if $B = \{v_{i}\}_{i=1}^{n}$ and $u = \sum_{i=1}^{n} a_{i}v_{i}$.

(a) Show that $\alpha \phi_{u} + \phi_{u'} = \phi_{\alpha u + u'}$. Conclude that the set $\{ \phi_{u} \}_{u \in V}$ forms a vector space over $F$.

(b) Show that the map $\phi_{u} : B \to F^{n}$ is equivariant for the actions of $B(a), B(b)$, in that for each $g \in \text{GL}_{n}(F), B \in B$, $g \left( \phi_{u}(B) \right) = \phi_{u}(gB)$.

(c) Physicists define a “covariant vector” to be an equivariant map $\phi : B \to F^{n}$. Let $\Phi$ be the set of covariant vectors. Show that the map $u \mapsto \phi_{u}$ defines an isomorphism $V \to \Phi$. (Hint: define a map $\Phi \to V$ by fixing a basis $B = \{v_{i}\}_{i=1}^{n}$ and mapping $\phi \mapsto \sum_{i=1}^{n} a_{i}v_{i}$ if $\phi(B) = a$).

(d) Physicists define a “contravariant vector” to be a map $\phi : B \to F^{n}$ such that $\phi(gB) = g^{-1} \cdot (\phi(B))$. Verify that $(g, a) \mapsto g^{-1} a$ defines an action of $\text{GL}_{n}(F)$ on $F^{n}$, that the set $\Phi'$ of contravariant vectors is a vector space, and that it is naturally isomorphic to the dual vector space $V'$ of $V$.

Supplementary Problems III: Fun in positive characteristic

E. Let $F$ be a field of characteristic 2 (that is, $1_{F} + 1_{F} = 0_{F}$).

(a) Show that for all $x, y \in F$ we have $x + x = 0_{F}$ and $(x + y)^{2} = x^{2} + y^{2}$.

(b) Considering $F$ as a vector space over $\mathbb{F}_{2}$ as in 5(a), show that the map $\text{Frob} : F \to F$ given by $\text{Frob}(x) = x^{2}$ is a linear map.

(c) Suppose that the map $x \mapsto x^{2}$ is actually $F$-linear and not only $\mathbb{F}_{2}$-linear. Show that $F = \mathbb{F}_{2}$. RMK Compare your answer with practice problem 1.

F. (This problem requires a bit of number theory) Now let $F$ have characteristic $p > 0$. Show that the Frobenius endomorphism $x \mapsto x^{p}$ is $\mathbb{F}_{p}$-linear.