Lior Silberman's Math 412: Problem Set 1 (due 18/1/2023)

Practice problems numbered M1 etc), any sub-parts marked "PRAC" (practice) "SUPP" (supplementary) and supplementary problems are not for submission.

Practice problems

M1. Show that the map $f\colon \mathbb{R}^3 \to \mathbb{R}$ 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 not.

M2. 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.

M3. For $x \in X$ let $\delta_x\colon F^X \to F$ be evaluation at x: $\delta_x(f) \stackrel{\text{def}}{=} f(x)$. Show that each δ_x is a linear map. Meditate on the fact that the vector space structure was defined exactly so that δ_x are linear maps.

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.

1. (Vector space axioms) Let $E = (E, 0_E, 1_E, +_E, \cdot_E)$ be a field, and let $F \subset E$ be a subfield, in other words a subset which is closed under the operations and satsifies the field axioms. It is commonly said that E naturally has the structure of an F-vectorspace.
   (a) Explicitely write the quadruple that was implicitely introduced in the statement of the problems.
   (b) Verify the vector space axioms for this putative vector space structure.
   (*Hint*: this problem is tedious rather than hard)

2. Let V be a vector space, $S \subset V$ a set of vectors. A *minimal dependence* in S is an equality $\sum_{i=1}^m a_i \underline{v}_i = \underline{0}$ where $\underline{v}_i \in S$ are distinct, a_i are scalars not all of which are zero, and $m \geq 1$ is as small as possible so that such $\{a_i\}$, $\{\underline{v}_i\}$ 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).
   PRAC Find a minimal dependence among $\left\{ \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}2\\1\\1\end{pmatrix} \right\} \subset \mathbb{R}^3$.
   (a) Show that in a minimal dependence the a_i are all non-zero.
   (b) Suppose that $\sum_{i=1}^m a_i \underline{v}_i$ and $\sum_{i=1}^m b_i \underline{v}_i$ are minimal dependences in S, involving the exact same set of vectors. Show that there is a non-zero scalar c such that $a_i = cb_i$.
   (c) Let $T\colon V \to V$ 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.
   (*d) Let Γ be a group. The set $\mathrm{Hom}(\Gamma, \mathbb{C}^\times)$ of group homomorphisms from Γ to the multiplicative group of nonzero complex numbers is called the set of *quasicharacters* of Γ (the notion of "character of a group" has an additional, different but related meaning, which is not at issue in this problem). Show that $\mathrm{Hom}(\Gamma, \mathbb{C}^\times)$ is linearly independent in the space $\mathbb{C}^\Gamma$ of functions from Γ to $\mathbb{C}$.

SUPP In the setting of problem 1, a *field homomorphism* is a map $\sigma\colon E \to E$ respecting the field operations. This map is an *automorphism* if it is invertible, equivalently if it is 1-1 and onto. Let $\mathrm{Aut}(E)$ be the set of field automorphisms of E, and let

$$\mathrm{Aut}_F(E) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma \restriction_F = \mathrm{id}_F\} .$$

(a) Show that $\mathrm{Aut}(E)$ is a group and that $\mathrm{Aut}_F(E)$ is a subgroup.

(b) Show that $\mathrm{Aut}(E) \subset E^E$ is linearly independent.
(*Hint*: See 2(d)).

(c) Thinking of E as an F-vectorspace as in problem 1, show that $\mathrm{Aut}_F(E) \subset \mathrm{Hom}_F(E,E)$. Use part (b) to show that $\mathrm{Aut}_F(E)$ is linearly independent, and conclude that $\#\mathrm{Aut}_F(E) \leq (\dim_F E)^2$ if $\dim_F E < \infty$.

RMK The integer $[E:F] = \dim_F E$ is usually called the *degree* of the field extension E/F. With more careful work it is possible to obtain the bound $\#\mathrm{Aut}_F(E) \leq [E:F]$.

3. (Matrices associated to linear maps) Let V,W be vector spaces of dimensions n,m respectively. Let $T \in \mathrm{Hom}(V,W)$ be a linear map from V to W. Show that there are ordered bases $B = \{\underline{v}_j\}_{j=1}^n \subset V$ and $C = \{\underline{w}_i\}_{i=1}^m \subset W$ 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

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

(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 $\iota\colon (\mathbb{Z},+) \to (F,+)$ by mapping $n \in \mathbb{Z}_{\geq 0}$ to the sum $1_F + \cdots + 1_F$ n times. Show that this extends to a ring homomorphism.

DEF If the map ι 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 ι. 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 ι 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. Show that there exists an integer $r \geq 1$ such that F has p^r elements.
(Hint: see problem 1)

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 $\dim_{\mathbb{Q}} V = 2d$.

Supplementary Problems II: How physicists define vectors

Fix a field F.

B. (The general linear group)
  (a) Let $\mathrm{GL}_n(F)$ denote the set of invertible $n \times n$ matrices with coefficients in F. Show that $\mathrm{GL}_n(F)$ forms a group with the operation of matrix multiplication.
  (b) For a vector space V over F let $\mathrm{GL}(V)$ denote the set of invertible linear maps from V to itself. Show that $\mathrm{GL}(V)$ forms a group with the operation of composition.
  (c) Suppose that $\dim_F V = n$ Show that $\mathrm{GL}_n(F) \simeq \mathrm{GL}(V)$ (hint: show that each of the two group is isomorphic to $\mathrm{GL}(F^n)$).

C. (Group actions) Let G be a group, X a set. An *action* of G on X is a map $\cdot\colon G \times X \to X$ 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 $(g, \underline{v}) \mapsto g\underline{v}$ defines an action of $G = \mathrm{GL}_n(F)$ on $X = F^n$.
  (b) Let V be an n-dimensional vector space over F, and let $\mathcal{B}$ be the set of ordered bases of V. For $g \in \mathrm{GL}_n(F)$ and $B = \{\underline{v}_i\}_{i=1}^{\dim V} \in \mathcal{B}$ set $gB = \left\{\sum_{j=1}^{n} g_{ij}\underline{v}_i\right\}_{j=1}^{n}$. Check that $gB \in \mathcal{B}$ and that $(g, B) \mapsto gB$ is an action of $\mathrm{GL}_n(F)$ on $\mathcal{B}$.
  (c) Show that the action is *transitive*: for any $B, B' \in \mathcal{B}$ there is $g \in \mathrm{GL}_n(F)$ 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 $\mathcal{B}$ be its set of bases. Given $\underline{u} \in V$ define a map $\phi_{\underline{u}}\colon \mathcal{B} \to F^n$ by setting $\phi_{\underline{u}}(B) = \underline{a}$ if $B = \{\underline{v}_i\}_{i=1}^{n}$ and $\underline{u} = \sum_{i=1}^{n} a_i \underline{v}_i$.
  (a) Show that $\alpha\phi_{\underline{u}} + \phi_{\underline{u}'} = \phi_{\alpha\underline{u}+\underline{u}'}$. Conclude that the set $\left\{\phi_{\underline{u}}\right\}_{\underline{u}\in V}$ forms a vector space over F.
  (b) Show that the map $\phi_{\underline{u}}\colon \mathcal{B} \to F^n$ is *equivariant* for the actions of B(a),B(b), in that for each $g \in \mathrm{GL}_n(F)$, $B \in \mathcal{B}$, $g\left(\phi_{\underline{u}}(B)\right) = \phi_{\underline{u}}(gB)$.
  (c) Physicists define a "covariant vector" to be an equivariant map $\phi\colon \mathcal{B} \to F^n$. Let Φ be the set of covariant vectors. Show that the map $\underline{u} \mapsto \phi_{\underline{u}}$ defines an isomorphism $V \to \Phi$. (Hint: define a map $\Phi \to V$ by fixing a basis $B = \{\underline{v}_i\}_{i=1}^{n}$ and mapping $\phi \mapsto \sum_{i=1}^{n} a_i \underline{v}_i$ if $\phi(B) = \underline{a}$).
  (d) Physicists define a "contravariant vector" to be a map $\phi\colon \mathcal{B} \to F^n$ such that $\phi(gB) = {}^t g^{-1} \cdot (\phi(B))$. Verify that $(g, \underline{a}) \mapsto {}^t g^{-1}\underline{a}$ defines an action of $\mathrm{GL}_n(F)$ on F^n, that the set Φ' 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 problem 5, show that the field automorphism $\mathrm{Frob}\colon F \to F$ given by $\mathrm{Frob}(x) = x^2$ is an $\mathbb{F}_2$-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.