Math 433, Fall 2006

Homework 1**, Selected Solutions**

§2, 4) The commutativity and associativity of addition and multiplication are clear from the tables. The same goes for the existence of additive and multiplicative identities (0 and 1 respectively). Again, studying the tables the additive inverses of 0 and 1 are, respectively, 0 and 1. The only nonzero element, namely 1, has a multiplicative inverse, itself. It remains to check the distributive law, that all $\alpha, \beta, \gamma \in F$, that $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$. This is clear for $\alpha = 0$, so we only need check it for $\alpha = 1$. That is we must verify that $1(\beta + \gamma) = 1\beta + 1\gamma$. This follows from the fact that 1 is the multiplicative indentity.

§2, 5) The commutativity, associativity and distributivity properties are inherited from $\mathbb{R}$.

We must show for any $p, q \in \mathbb{Q}$ that $p + q \in \mathbb{Q}$, $pq \in \mathbb{Q}$, $-p \in \mathbb{Q}$ and $1/p \in \mathbb{Q}$. We must also show $0, 1 \in \mathbb{Q}$. These are clear or follow from exercise 2).

§4, 3) a), c), e), f) and g) are subspaces. These sets are closed under addition and scalar multiplication. (Note b) is closed under *rational* scalar multiplication, but not under real scalar multiplication.

§4, 10) Let $m > n$ and suppose $\{\vec{v}_1, ..., \vec{v}_n\}$ is dependent. We must prove $\{\vec{v}_1, ..., \vec{v}_m\}$ is dependent. Consider the dependence relation $\sum_{i=1}^{n} \alpha_i \vec{v}_i = \vec{0}$. We know that some $\alpha_i \neq 0$, say $\alpha_{i_0} \neq 0$. For $i \leq n$ set $\beta_i = \alpha_i$. For $n + 1 \leq i \leq m$ set $\beta_i = 0$. Then $\sum_{i=1}^{m} \beta_i \vec{v}_i = \vec{0}$ is a dependence relation for $\{\vec{v}_1, ..., \vec{v}_m\}$ with $\beta_{i_0} \neq 0$.

An analogous statement is: Show that a set of vectors that is contained in a linearly independent set of vectors is itself linearly independent.

§5, 5) If $\sum_{i=1}^{m} \alpha_i \vec{v}_i = \sum_{i=1}^{m} \alpha_i' \vec{v}_i$ then we have

$$\sum_{i=1}^{m} \alpha_i \vec{v}_i - \sum_{i=1}^{m} \alpha_i' \vec{v}_i = \sum_{i=1}^{m} (\alpha_i - \alpha_i') \vec{v}_i = \vec{0}.$$

The independence of the set $\{\vec{v}_1, ..., \vec{v}_m\}$ implies that for all i we have $\alpha_i - \alpha_i' = 0$, that is, for all i, we have $\alpha_i = \alpha_i'$.

§6, 1 a) Subtracting the first row and twice the first row from the second and third rows respectively gives $\begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & -1 & -2 & -1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ which is in echelon form.

b) Subtracting the first row from the third row gives $\begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & -1 \\ 0 & 1 & 2 \end{bmatrix}$. Now we add $-.5$ times the second row of this matrix to the third row to get $\begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & -1 \\ 0 & 0 & 2.5 \end{bmatrix}$ which is in echelon form.

c) Subtracting the 1.5 times the first row from the second row gives $\begin{bmatrix} 2 & -1 & 1 & 2 \\ 0 & 1.5 & -.5 & -2 \\ 0 & 3 & -1 & -4 \end{bmatrix}$.

Now we subtract twice the second row of this matrix from the third row to get $\begin{bmatrix} 2 & -1 & 1 & 2 \\ 0 & 1.5 & -.5 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

Also:

1) Let $S(n)$ be the statement $\sum_{k=1}^{n} k^3 = \left(\frac{k(k+1)}{2}\right)^2$. Our goal is to prove the truth of the statement $S(n)$ for all natural numbers n by induction. For $n = 1$ both the left and right hand sides are 1. We have verified the truth of the statement $S(1)$. Suppose $S(r-1)$ is true. Then we have

$$\sum_{k=1}^{r} k^3 = r^3 + \sum_{k=1}^{r-1} k^3 = r^3 + \left(\frac{(r-1)(r-1+1)}{2}\right)^2 = \left(\frac{r(r+1)}{2}\right)^2.$$

Thus $S(r)$ is true. By induction we have the truth of the statement $S(n)$ for all natural numbers n.

2) The second equation gives $x = y$, whether we are working over $\mathbb{R}$ or $\mathbb{F}_2$. Substituting this into the first equation gives $2x = 0$. This is also independent of the field. Over $\mathbb{R}$ we divide by 2 to get $x = 0$, and then $y = 0$. So $(0, 0)$ is the only solution to the sytem over $\mathbb{R}$.

Over $\mathbb{F}_2$ we have that $2 = 1 + 1 = 0$, so the equation $2x = 0$ becomes $0 = 0$. In $\mathbb{F}_2$ we have that $1 = -1$ so the two equations are the same! Thus we need only solve the second equation $x = y$. The only solutions to the system over $\mathbb{F}_2$ are $(0, 0)$ and $(1, 1)$.

3) a) Write $m = ab$ where $a, b \in \mathbb{N}$ and $a, b > 1$. If $\mathbb{Z}/m\mathbb{Z}$ is a field then a has an inverse in $\mathbb{Z}/m\mathbb{Z}$. Let x be the inverse. Then $xa = 1$ in $\mathbb{Z}/m\mathbb{Z}$, that is $xa - 1$ is divisible by $m = ab$ in $\mathbb{Z}$. Then $xa - 1$ is divisible by a, so -1 is divisible by a, a contradiction.

b) We only need to prove the existence of multiplicative inverses. Let p be a prime and choose $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. We show the 'multiplication by a' map from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ given by $x \mapsto ax$ is injective. Suppose there are elements $y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $ay = az$ in $\mathbb{Z}/p\mathbb{Z}$, that is $ay - az$ is a multiple of p. But since $a \neq 0$, we see a is not a multiple of p so $x - y$ is a multiple of p so $x = y$ in $\mathbb{Z}/p\mathbb{Z}$. This proves the injectivity. But the domain and range of the 'multiplication by a' are both $\mathbb{Z}/p\mathbb{Z}$. Thus the injectivity of the 'multiplication by a map' implies its surjectivity. Let $a_0 \in \mathbb{Z}/p\mathbb{Z}$ be the unique element such that $aa_0 = 1$ in $\mathbb{Z}/p\mathbb{Z}$. Then a_0 is the multiplicative inverse of a.

4) We need the lemma below.

Lemma Let V be a vector space over a field $\mathbb{F}$ and W a subspace of V. If W is not finitely generated then V is not finitely generated.

Proof: We proceed by contradiction. We are given that W is not finitely generated and suppose that V is finitely generated, say by $\{\vec{v}_1, ..., \vec{v}_m\}$. Since W is not finitely generated, it is not the zero subspace of V. Thus we can choose a non-zero $\vec{w}_1 \in W$. Let W_1 be the subspace of W generated by $\vec{w}_1$. Then $W_1 \neq W$ as W is not finitely generated. Thus there is a $\vec{w}_2 \in W \backslash W_1$. The set $\{\vec{w}_1, \vec{w}_2\}$ is independent. (Why?) Let W_2 be the subspace of W generated by $\{\vec{w}_1, \vec{w}_2\}$. Then $W_2 \neq W$ as W is not finitely generated. Thus there is a $\vec{w}_3 \in W \backslash W_1$. The set $\{\vec{w}_1, \vec{w}_2, \vec{w}_3\}$ is independent. (Again, why?) Continuing in this fashion, we can construct an independent set $\{\vec{w}_1, ..., \vec{w}_{m+1}\} \subset W \subset V$. But V is generated by $\{\vec{v}_1, ..., \vec{v}_m\}$. We have a contradiction with Theorem (5.1) of the text. Thus V is not finitely generated. The proof of the lemma is complete.

Remark If A and B are statements (like for example '$n > 2$ is prime' and '$n > 2$ is odd') then maybe one can prove $A \Rightarrow B$. If you are able to prove this implication, then you have also proven the contrapositive: $\sim A \Rightarrow \sim B$, where $\sim X$ denotes the negation of the statement X. Thus we have also proved
Lemma Let V be a vector space over a field $\mathbb{F}$ and W a subspace of V. If V is finitely generated then W is finitely generated.

Let's answer the question. The problem is $D^\infty(\mathbb{R})$ contains lots of complicated functions and is hard to 'get a hold of'. We work with the subspace $\mathcal{P}$ of polynomials. We will show $\mathcal{P}$ is not finitely generated. The lemma then implies $D^\infty(\mathbb{R})$ is not finitely generated.

We proceed by contradiction. Suppose $\mathcal{P}$ is finitely generated, say by $\{f_1(x), ...f_n(x)\}$. Let d be the maximum of the degrees of the polynomials $f_i(x)$, $1 \leq i \leq n$. Then $g(x) = x^{d+1}$ is not in the span of $\{f_1(x), ...f_n(x)\}$. Thus $\mathcal{P}$ is not finitely generated.

5) A union of subspaces need not be a subspace. Consider $V = \mathbb{R}^2$ and V_1 and V_2 being the x and y axes respectively. Then each v_i is a subspace, but $V_1 \cup V_2$ is not closed under addition, hence not a subspace.

An intersection of subspaces is a subspace. Indeed, let $\vec{u}, \vec{v} \in \cap_\alpha V_\alpha$ and $a \in F$. Then for each α we have $\vec{u}, \vec{v} \in V_\alpha$ so $\vec{u} + a\vec{v} \in V_\alpha$ as V_α is a subspace of V. Thus $\vec{u} + a\vec{v} \in \cap_\alpha V_\alpha$, so $\cap_\alpha V_\alpha$ is a subspace of V.

6) Let $\alpha \in \mathbb{R}$ and let $f(x), h(x) \in D^\infty(\mathbb{R})$ be solutions to $dg/dt = g$. Thus $df/dt = f$, $dh/dt = h$. We easily see $d(f + \alpha h)/dt = (f + \alpha h)$. The set of solutions to $dg/dt = g$ that are in $D^\infty(\mathbb{R})$ form a subspace of $D^\infty(\mathbb{R})$

It is an elementary result in the theory of differential equations that for any real number A, the function $g(x) = Ae^x$ satisfies $dg/dt = g$ and all solutions are of this form. Thus the subspace of solutions is finitely generated by one element of $D^\infty(\mathbb{R})$ and is one dimensional.