Math 100b Winter 2010 Homework 7

Due 3/5/09 in class, or by 5pm in HW box on 6th floor of AP&M

1. Suppose that F is a field with finitely many elements. First show that F has characteristic p for some prime $p > 0$. Then there is an injective ring homomorphism $\phi : \mathbb{Z}_p \to F$ defined by $[n] \mapsto n \cdot 1$, and in this way we see that F contains a subfield, namely $\operatorname{Im} \phi$, which is isomorphic to $\mathbb{Z}_p$. Informally we just identify $\operatorname{Im} \phi$ with $\mathbb{Z}_p$ and so think of $\mathbb{Z}_p$ as a subfield of F, called the prime subfield.

By considering F as a vector space over $\mathbb{Z}_p$, show that $|F| = p^n$ for some $n \geq 1$.

Remark. This shows that every finite field has a prime-power number of elements. In Math 100c, you will see that for every prime power p^n, there is exactly one field with that number of elements (up to isomorphism.)

2. Prove the following "replacement lemma", which shows that given a finite basis of a vector space and any nonzero vector w, some basis element can be replaced by w yielding another basis.

Lemma 0.1 *Let V be a vector space over a field F, such that $\{v_1, v_2, \ldots, v_n\}$ is a basis for V. Suppose that $0 \neq w \in V$ is a nonzero vector, and write $w = a_1 v_1 + \cdots + a_n v_n$ for some $a_i \in F$. Suppose that i is any index such that $a_i \neq 0$. Prove that $\{v_1, v_2, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n\}$ is also a basis for V.*

3. In class, we defined $\dim_F V$ to be the number of elements in a basis for V as a vector space over F. (Recall that we usually just write $\dim_F V = \infty$ if this number is infinite, and will not concern ourselves too much with the cardinality of infinite sets.) In this problem, you will show that this concept of dimension is well-defined. The main work is in part (a) below; the other parts all follow quickly from part (a).

(a). Let V be a vector space over a field F with basis $\{v_1, v_2, \ldots, v_n\}$. Suppose that $\{w_1, w_2, \ldots, w_m\}$ is a linearly independent set of vectors in V with $m \leq n$. Show that, possibly after rearranging the order of the basis vectors v_i, then $\{w_1, w_2, \ldots, w_i, v_{i+1}, \ldots, v_n\}$ is again a basis of V for all

$1 \le i \le m$. In other words, we can replace the elements of the basis $\{v_i\}$ one by one with the w_i and still have a basis.

(Hint: induction on i. Use the replacement lemma from problem 2 in the induction step.)

(b). Show that if V has a basis with n elements, then any linearly independent set of vectors in V contains at most n vectors. (Hint: If S is a set of more than n independent vectors, using part (a) you can show that that first n of them are already a basis; achieve a contradiction.)

(c). Show that if V has a finite basis, then any linearly independent set of vectors in V is contained in some basis of V.

(d). Show that if V has a finite basis with n elements, then every basis of V is also finite and has n elements. This completes the proof that $\dim_F V$ is well-defined.

4. Suppose V is a vector space over F with basis S (which might be infinite). Note that the sum $\sum_{v \in S} a_v v$ makes sense (even if S is infinite), as long as only finitely many of the scalars $a_v \in F$ are nonzero; this is really a linear combination of finitely many vectors because the ones with zero coefficient aren't "really there". (Note that we are using the notation a_v for the coefficient of the basis vector v; it may seem weird to use a vector as a subscript but this is useful because then the subscript indicates which vector the coefficient is attached to.)

(a). Show that every element $w \in V$ has a *unique* expression of the form $w = \sum_{v \in S} a_v v$ (where $a_v \neq 0$ for only finitely many $v \in S$). In other words, the coefficients a_v are uniquely determined by w.

(b). Let W be any other vector space over F. Show that given any function $f : S \to W$, there is a unique linear transformation $\phi : V \to W$ such that $\phi(s) = f(s)$ for all $s \in S$.

Remark: In words, this says that to define a linear transformation, it is enough to say where we send the elements of a basis, and moreover we can send them anywhere we please. V is said to be free *on the basis S because there is no restriction on where a homomorphism sends the elements in S.*

(c). Recall that F^n is the vector space $\{(b_1, \dots, b_n) | b_i \in F\}$ of n-tuples of elements of F. Let V be any vector space with $\dim_F V = n$. Show that $V \cong F^n$ as vector spaces, in other words there is a bijective linear transformation $\phi : V \to F^n$. Thus all vector spaces of dimension n are isomorphic.

5. Let V be the set of all functions $f : \mathbb{R} \to \mathbb{R}$, which is a vector space over $\mathbb{R}$ with pointwise defined addition $[f + g](x) = f(x) + g(x)$ and scalar multiplication $[af](x) = af(x)$.

Show that $\dim_F V = \infty$. (Hint: construct an infinite linearly independent subset of V, and then quote problem 3. Note that your functions are not required to be continuous.)

Remarks: In fact, for students that know the theory of countability, it is not any harder to find an uncountable linearly independent set of vectors; this shows that in fact any basis for V is uncountable, because it is true in general that any set of linearly independent vectors has cardinality at most as large as the cardinality of a basis. In analysis one might be more interested in the vector space of all continuous *functions $f : \mathbb{R} \to \mathbb{R}$, or even the vector space of all infinitely-differentiable functions $f : \mathbb{R} \to \mathbb{R}$. These vector spaces also have uncountable dimension, as you might be interested in trying to show.*

6. Let $R = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 | a, b, c \in \mathbb{Q}\} \subseteq \mathbb{R}$. It is not hard to check that R is a subring of $\mathbb{R}$; you can just assume this.

Prove that $R \cong \mathbb{Q}[x]/\langle x^3 - 2\rangle$ (as rings). Conclude that R is a field. Also, clearly R contains $\mathbb{Q}$ as a subfield, so we can think of R as a vector space over $\mathbb{Q}$. Show that $\dim_{\mathbb{Q}} R = 3$.