Math 342 Problem set 8 (due 11/3/09)

Rings and vector spaces

1. Let R be a ring. We define a map $f\colon \mathbb{N} \to R$ inductively by $f(0) = 0_R$ and $f(n+1) = f(n) + 1_R$.
   (a) Show that $f(1) = 1_R$. Show that $f(n+m) = f(n) + f(m)$ for all $n,m \in \mathbb{N}$.
   Hint: Induction on m.
   (b) Show that f respects multiplication, that is for all $n,m \in \mathbb{N}$, $f(nm) = f(n) \cdot f(m)$.
   Hint: Induction again. The case $m = 0$ uses a result from class.
   SUPP Extend f to a function $g\colon \mathbb{Z} \to R$ by setting $g(n) = f(n)$ if $n \in \mathbb{Z}_{\geq 0}$, and $g(n) = -f(-n)$ if $n \in \mathbb{Z}_{\leq 0}$. Show that g is a ring homomorphism.
   Hint: Divide into cases.

*2. Let E be a field, and let $F \subset E$ be a *subfield* (F contains $0_E, 1_E$, and is closed under addition, multiplication, negatives and inverses). Consider the set E with the following two operations: addition in E and multiplying elements of E by elements of F. Show that this makes E into a vector space over F.
Hint: You need to go over the axioms in Definition 79 and deduce them from what you know about E due to Definition 58.

Linear algebra

3. In each case, check whether the vector is linearly dependent on the other vectors. If it is, exhibit it as a linear combination. If not, prove that this cannot be done.
   (a) $(1,2,3)$ on $\{(2,4,0), (0,0,1), (0,0,0)\}$ in $\mathbb{R}^3$?
   (b) $(5,7,-2)$ on $\{(3,2,1), (1,0,0)\}$ in $\mathbb{R}^3$.
   (c) $([5]_{11}, [7]_{11}, [-2]_{11})$ on $\{([3]_{11}, [2]_{11}, [1]_{11}), ([1]_{11}, [0]_{11}, [0]_{11})\}$ in $\mathbb{F}_{11}^3$ (for a prime p, $\mathbb{F}_p$ is another notation for the field $\mathbb{Z}/p\mathbb{Z}$).
   (d) The polynomial $[5]_7 x + [1]_7$ on $\left\{[2]_7 x^2 + [1]_7 x, x^2 + [5]_7 x + [3]_7\right\}$ in the space of polynomials over $\mathbb{F}_7$.

*4. Let F be a field, V a vector space over F, and let $B = \{\underline{v}_i\}_{i=1}^n \subset V$ be a linearly independent subset of V which spans V. Consider the map $f\colon F^n \to V$ given by $f(x_1, \ldots, x_n) = \sum_{i=1}^n x_i \underline{v}_i$.
   (a) Show that f is a linear map.
   (b) Show that f is *onto*, that is that the image f is the whole of V.
   Hint: What is the definition of "span"?
   (c) Show that f is *injective*, that is that if $\underline{x} \neq \underline{y}$ in F^n then $f(\underline{x}) \neq f(\underline{y})$ in V.
   Hint: Assume $f(\underline{x}) = f(\underline{y})$, subtract $f(\underline{y})$ from both sides, and use the definition of independence to show $\underline{x} = \underline{y}$.
   (d) Conclude that every n-dimensional vector space over F is isomorphic to F^n.

REMARK 94. This is why the case of F^n is the one most studied.

The Hamming Code (variant)

5. Let $H \in M_{3\times 7}(\mathbb{F}_2)$ be the matrix whose columns are all non-zero vectors in $\mathbb{F}_2^3$, that is

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

   (a) Let $a,b,c,d \in \mathbb{F}_2$be a 4-bit "message" we want to transmit. Show that there exist unique $x,y,z \in \mathbb{F}_2$ so that $H \cdot (x,y,z,a,b,c,d)^T = \underline{0}$. We will trasmit the redundant 7-bit vector instead.
   Hint: Need to show both that x,y,z exist and that they are unique. Express the problem as a system of linear equations over $\mathbb{F}_2$.

   (b) For each $1 \le i \le 7$, let $\underline{e}^i$ be the standard basis vector of $\mathbb{F}_2^7$ with 1 at the ith co-ordinate. Calculate the seven vectors $H\underline{e}^i$.

   (c) Let $\underline{v}, \underline{v}' \in \mathbb{F}_2^7$ be at Hamming distance 1. Show that there exists i so that $\underline{v}' = \underline{v} + \underline{e}^i$.

   (d) Now let's say Alice transmits the 7-bit vector $\underline{v} = (x,y,z,a,b,c,d)^T$ from part (a), through a channel that can change at most one bit in every seven. Denote by $\underline{v}'$ the 7 bits Bob receives, and show that if $\underline{v}' \neq \underline{v}$ then $H\underline{v}' \neq \underline{0}$. Conclude that Bob can detect if a 1-bit error occured.
   Hint: Use the fact that $H\underline{v} = \underline{0}$ and your answers to parts (c) and (b).

   (e) In fact, if at most one bit error can occur then Bob can *correct* the error. Using the fact that the vectors $H\underline{e}^i$ are all different (see your answer to part (b)), show that knowing only $\underline{v}'$ and that at most one error occured, he can calculate the difference $\underline{e} = \underline{v}' - \underline{v}$ and hence the original vector $\underline{v}$.
   Hint: What are the possibilities for $\underline{e}$? For $H\underline{e}$? how do they match up? Don't forget that it's possible that $\underline{v}' = \underline{v}$.

Supplementary problems

A (Prime fields and finite fields)

   (a) Let g be the map from 1(c). Show that $\mathrm{Ker}(g)$ is an ideal of $\mathbb{Z}$.

   (b) Let E be a field, and let $g\colon \mathbb{Z} \to E$ be the map from problem 1. Show that $\mathrm{Ker}(g) = (p)$ where $p = 0$ or p is prime.
   Hint: If $m = ab$ apply g to both sides.

   (c) Conclude that every finite field contains a copy of $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ for a prime p.

   (d) Show that every finite field has p^n elements for some n.

REMARK. It is also true that for every $q = p^n$ there exists a field $\mathbb{F}_q$ of size q, unique up to isomorphism.