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

Prime rings

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.
   OPTIONAL 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 A, B be rings and $g\colon A \to B$ be a homomorphism. Show that the image $g(A) = \{b \in B \mid \exists a \in A : g(a) = b\}$ is a subring of B.

3. Continuing problem 1, let g be the ring homomorphism you constructed, let $S = g(\mathbb{Z})$ be the image of g, and let $I = g^{-1}(0_R)$ be the set of $n \in \mathbb{Z}$ such that $g(n) = 0_R$.
   (a) Show that I is an ideal in $\mathbb{Z}$. By a previous problem set there is $m \in \mathbb{N}$ such that $I = (m)$.
   (b) If $m = 0$ show that g is injective, hence that R contains a subring isomorphic to $\mathbb{Z}$.
   Hint: Use the criterion for injectivity from problem set 7.
   (c) Show that $m = 1$ is impossible, as long as $0_R \neq 1_R$.
   Hint: What is $g(1)$ if $m = 1$? Compare with problem 1(a).
   (d) If $m \geq 2$, define $h\colon \mathbb{Z}/m\mathbb{Z} \to R$ by $h([a]_m) = g(a)$. Show that h is a well-defined function (that is, if $[a]_m = [a']_m$then $g(a) = g(a')$).
   (e) Show that h is a ring homomorphism.
   (f) Show that h is an isomorphism.
   Hint: To check injectivity, it is enough to understand $h([0]_m)$; to check surjectivity, given $s \in S$ need to find $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $h([a]_m) = s$.
   We conclude that every ring contains either a subring isomorphic to $\mathbb{Z}$ or a subring isomorphic to $\mathbb{Z}/m\mathbb{Z}$ for some $m \geq 2$.

REMARK. You can also check that $S = g(\mathbb{Z})$ is the smallest subring of R – the intersection of all subrings of R.

Prime fields and vector spaces

Now let F be a field, and let $g\colon \mathbb{Z} \to F$ be the map constructed in problem 1. Let m be the number defined in problem 3.

4. Assume by contradiction that m is positive and composite, that is $m = ab$ with $1 < a, b < m$. Apply the function g and obtain a contradiction to the fact that F is a field. Conclude that either $m = 0$ or m is prime.

DEFINITION. m is called the *characteristic* of the field F and denoted $\mathrm{char}(F)$. Problems 1-4 now show that the characteristic of a field is either zero or a prime number, and that a field of prime characteristic p contains an isomorphic copy of $\mathbb{F}_p$.

5. Let F be a finite field.
   (a) Show that $\mathrm{char}(F) > 0$. Conclude that $\mathbb{F}_p \subset F$ for some p.
   Hint: You need to rule out $\mathrm{char}(F) = 0$; for this use problem 3(b).
   (b) Show that F has the structure of a vector space over $\mathbb{F}_p$.
   Hint: All the vector space axioms follow directly from the field axioms.
   (c) Show that $\dim_{\mathbb{F}_p} F < \infty$ (can F contain an infinite linearly independent set?). It follows that, as an $\mathbb{F}_p$-vector space, F is isomorphic to $\mathbb{F}_p^n$ for some $n \geq 1$.
   (d) Show that the number of elements of a finite field is always a prime power.
   Hint: How many elements are there in $\mathbb{F}_p^n$?

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.

The Hamming Code (variant)

6. (§13E.E6) 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.
   (b) For each $1 \leq i \leq 7$, 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 we transmit 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 received bits, and show that if $\underline{v}' \neq \underline{v}$ then $H\underline{v}' \neq \underline{0}$. Conclude that the recipient 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 the recipient 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, the recipient 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 $\underline{v}' = \underline{v}$.