Math 412/512 Assignment 7

Due Monday, December 12

1) Recall the definition provided in class of a field with 4 elements: Given $\{0, 1, x, y\}$, the operations "+" and $\cdot$ were determined by the following tables.

$\cdot$	*0*	*1*	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

$+$	*0*	*1*	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

Complete the proof that this is a field by showing distributivity.

2) For a unital ring R, let $R^\times$ denote the set of all units.

a) Prove that $(R^\times, \cdot)$ is a group, where "$\cdot$" is the multiplication operation on R.

b) Determine the group isomorphism class of $\mathbb{Z}[x]^\times$.

c) If R and S are unital rings, determine $(R \oplus S)^\times$ as a subset of $R \oplus S$.

3) Check that the following subrings of the given rings are actually ideals.

a) $\{p \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$

b) $\{n \in \mathbb{Z}_8 \mid n \notin \mathbb{Z}_8^\times\}$

c) $\{f \in C_0(\mathbb{R}) \mid f(x) = 0 \ \forall\ x \in \mathbb{Q}\}$

4) Check that the following commutative rings are actually fields.

a) $\left\{x \in M_2(\mathbb{R}) \mid x = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right\}$, inherited operations from $M_2(\mathbb{R})$.

b) $\{a + b\sqrt{15} \mid a, b \in \mathbb{Q}\}$, inherited operations from $\mathbb{R}$.

c) $\{n+im \mid n,m \in \mathbb{Z}_7,\ i^2=-1\}$, operations

$$(n+im)\cdot(a+ib) = (an-mb)\text{mod}(7) + i((nb+ma)\text{mod}(7))$$

and

$$(n+im)+(a+ib) = (n+a)\text{mod}(7) + i((m+b)\text{mod}(7))$$

.

5) Let I be an ideal in the ring R and J be an ideal in the ring S. Prove that $I \oplus J$ is an ideal in $R \oplus S$.

6) (#58, Chapter 13) Let F be a finite field with n elements. Prove that $x^{n-1} = 1_F$ for all nonzero $x \in F$.

7) (#18, Chapter 19) Let $P = \{(a,b,c) \mid a,b,c \in \mathbb{R},\ a = 2b+3c\}$. Prove that P is a subspace of $\mathbb{R}^3$. Find a basis for P.

8) a) Show that $C(\mathbb{R})$ is a vector space over $\mathbb{R}$.

b) Prove that $C(\mathbb{R})$ is infinite dimensional as a vector space over $\mathbb{R}$.

9) Establish that $\mathbb{Q}(\sqrt{5},\sqrt{7}) = \mathbb{Q}(\sqrt{5}+\sqrt{7})$.

Extra Credit Problem

Directions: I will accept no written solutions for even a part of the following problem. They must be proved on a blackboard with me listening to the proof.

1) (Grassmannians) For a field F and a vector space V over F, the *Grassmannian* $Gr(k, V)$ is the collection of all k-dimensional linear subspaces of V. The *order* of $Gr(k, V)$ is the number of distinct k-dimensional linear subspaces of V.

a) Determine, with proof, the number of distinct one-dimensional subspaces of $\mathbb{Z}_p^n$, i.e., find the order of $Gr(1, \mathbb{Z}_p^n)$.

b) The order of $Gr(k, \mathbb{Z}_p^n)$ for $k \leq n$ is given by the formula $\dfrac{[n]_p!}{[n-k]_p![k]_p!}$ where for $m \in \mathbb{N}$,

$$[m]_p = \frac{p^m - 1}{p - 1}$$

and $[m]_p!$ is defined by

$$[m]_p! = [m]_p \cdot [m-1]_p \cdots [2]_p \cdot [1]_p.$$

Compute $\dfrac{[n]_p!}{[n-k]_p![k]_p!}$ for arbitrary p, n, and k, then take the limit as $p \to 1$. Ruminate on your answer and you may start to get some idea of what people mean by "the field with one element."

c) Actually prove that the order of $Gr(k, \mathbb{Z}_p^n) = \dfrac{[n]_p!}{[n-k]_p![k]_p!}$ for $1 < k < n$.

2) Provide, with proof, an example of a ring R with no zero divisors where $x^2 = y^2$ does not necessarily imply either $x = y$ or $x = -y$ for $x, y \in R$.