Math 412/512 Assignment 8

Due Friday, April 15

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) (See Chapter 29, Section B in Pinter) Let $n, m \in \mathbb{N}$ and suppose $n \neq m$.

a) Find polynomials $p, q, r \in \mathbb{Z}[x]$ such that $p(\sqrt{5} + \sqrt{7}) = q(\sqrt{5}) = r(\sqrt{7}) = 0$.

b) Prove that $\mathbb{Q}[\sqrt{n}, \sqrt{m}] = \mathbb{Q}[\sqrt{n} + \sqrt{m}]$.

c) Compute the degree of $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$, with a proof that your answer is correct.

d) Show that $\mathbb{Q}[\sqrt{7}]$ and $\mathbb{Q}[\sqrt{5}]$ are not isomorphic as fields. *Hint:* Prove that any isomorphism is the identity on $\mathbb{Q}$ and argue by contradiction.

3) If F is a field and E an extension field of F. Let $A \subset E$ denote all elements of E that are algebraic over F. Prove that A is a subfield of E.

4) a) Let R be a unital commutative ring. Show that R/I is a field if and only if I is maximal.

b) Give an example, with proof, of a noncommutative unital ring R and a maximal ideal I in R where R/I is not a field.

5) 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) Compute the number of elements in $\mathbb{Z}_p^n$ where p is a prime number. Be sure to prove your answer is correct.

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

c) 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."

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