November 4th, 2009

Math 351

Luís Finotti
Fall 2009

Name: .....

Student ID (last 6 digits): XXX- .....

Midterm 2 (Take Home)

You must turn in this exam in class on Wednesday, November 4th. Since this is a take home, I want all your solutions to be neat and well written.

You do *not* need to do part (a) of a question to use it in part (b)!

Do all work on this exam, i.e., on the page of the respective assignment, or you can add pages if yon need more space.

Write your name and the last six digits of your student ID number on the top of this page. Check your exam has 4 questions.

You can look at your notes and at our book, but you cannot look at any other references (including the Internet) and you cannot discuss this with *anyone*!

Good luck!

Question	Max. Points	Score
1	25	
2	25	
3	25	
4	25	
Total	100	

1) [25 points] Let K be a field and $F \subseteq K$. Suppose that F is also a field with the *same addition and product* as K. [We are *not* assuming that $1_k = 1_F$, so, in principle, F might now be a subfield of K.]

(a) Show that $1_F \neq 0_K$. [**Hint:** Remember that since F is a field, $1_F \neq 0_F$.]

(b) Show that $1_F = 1_K$. [**Hint:** By part (a), 1_F is invertible in K, and so if $1_F \cdot a = 1_F \cdot b$, for any $a, b \in K$ [or F], we have that $a = b$.]

2) [25 points] Let R be a [not necessarily commutative] ring [with one] such that $a^2 = a$ for all $a \in R$.

(a) Show that $1_R = -1_R$. [**Hint:** Consider $(1_R + 1_R)^2$.]

(b) Show that R is commutative. [**Hint:** By (a), it suffices to show that for all $a, b \in R$, we have $ab + ba = 0$. Consider $(a + b)^2$, and remember we cannot assume that R is commutative!]

3) [25 points] Let p be a prime with $p \geq 3$, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ [or $\mathbb{F}_p = \mathbb{I}_p$, as in the book]. [Remember that $\mathbb{F}_p$ is a *field*!] Let $U = \mathbb{F}_p^\times$ be the set of units of $\mathbb{F}_p$.

(a) Show that the only elements of $a \in \mathbb{F}_p^\times$ such that $a = a^{-1}$ are $\overline{1}$ and $\overline{p-1}$. [**Hint:** If $a^{-1} = a$, then $a^2 = \overline{1}$. Then, what are all the roots of the polynomial $x^2 - \overline{1}$ in $\mathbb{F}_p$?]

(b) Use (a) to show that $(p-1)! \equiv -1 \pmod{p}$. [**Hint:** That is the same as to say that $\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{p-1}$.]

4) [25 points] Let R be an *integral domain*, and suppose that there is some $n \in \mathbb{Z} \setminus \{0\}$ such that $n \cdot 1_R = 0_R$. [Note that n can be negative.]

(a) Show that there exists some prime p such that $p \cdot 1_R = 0_R$. [**Hint:** We have that if $a, b \in \mathbb{Z}$, then $(a \cdot b) \cdot 1_R = (a \cdot 1_R) \cdot (b \cdot 1_R)$. Then, use the *Fundamental Theorem of Arithmetic* and the fact that R is a domain.]

(b) Show that the prime in (a) is unique. [**Hint:** If $p \neq q$, both primes, then $\gcd(p, q) = 1$. You can use *Bezout's Theorem* [i.e., the *Extended Euclidean Algorithm*]. Also, remember that $1_R \neq 0_R$.]