Homework #1. Due on Friday, January 29th, by 3pm in my mailbox

Reading:

1. For this assignment: Online lectures 1 and 2.
2. For next week's classes: Online lectures 2 and 3.

Online lectures are currently posted on last year's webpage

`http://people.virginia.edu/~mve2x/3354_Spring2015`

Additional reading assignments from Pinter's and Gilbert's books will be posted later.

Problems:

Problem 1: Let R be a commutative ring with 1. Prove the following equalities using only the ring axioms and results proved in class or online lectures.

(a) $-(-x) = x$ for all $x \in R$
(b) $(-1)(-1) = 1$
(c) $(-x)(-y) = xy$ for all $x, y \in R$
(d) $x(y - z) = xy - xz$ for all $x, y, z \in R$

Hint: Additive cancellation law (proved in lecture 1) can be used to solve many questions of this type as follows. Suppose that we want to prove inequality of the from $a = b$. By additive cancellation law, if we prove that $a + c = b + c$ for some $c \in R$, we can conclude that $a = b$. Note that the implication would work for any c, so c is for us to choose. The idea is to choose c in such a way that both expressions $a+c$ and $b+c$ can be simplified (using ring axioms) so that after simplification it becomes easy to prove that $a + c = b + c$.

Recall that by definition $x - y = x + (-y)$.

Problem 2: Let F be a field, and suppose that $xy = 0$ for some $x, y \in F$. Prove that $x = 0$ or $y = 0$. **Hint:** Consider two cases: $x = 0$ (in this case there is nothing to prove) and $x \neq 0$. Recall that in a field every nonzero element has multiplicative inverse.

Note: If F was only assumed to be a commutative ring with unity, the above assertion would have been false in general. Can you think of an example?

Problem 3: Let R be an ordered ring and $x, y, z \in R$. Prove that

(a) If $x > y$, then $x + z > y + z$
(b) If $x > y$ and $z > 0$, then $xz > yz$

(c) If $x > y$ and $z < 0$, then $xz < yz$

Note: You may use freely standard properties of ring operations (addition, subtraction and multiplication). However, all statement involving inequalities must be deduced directly from the axioms.

Problem 4: Let X be any set, and let $R = \mathcal{P}(X)$ (the power set of X), that is, R is the of all subsets of X. As in online lecture 2, define addition $+$ and multiplication $\cdot$ on R by setting $A \cdot B = A \cap B$ (intersection) and $A + B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$ (symmetric difference ='exclusive or') for arbitrary $A, B \in R$ (that is, for arbitrary $A, B \subseteq X$). Prove that R with these operations is a commutative ring with 1.

Note: Multiplication axioms (M0)-(M3) are checked in online lecture 3, so you only need to check the addition axioms (A0)-(A4) and distributivity.

Hint: To check associativity of addition ($(A+B)+C = A+(B+C)$), take an arbitrary element $x \in X$, and consider 8 cases: case 1 ($x \in A$, $x \in B$, $x \in C$), case 2 ($x \in A$, $x \in B$, $x \notin C$) etc. In each case show that x belongs to both $(A+B)+C$ and $A+(B+C)$ or does not belong to either of those sets.

Problem 5: The following question is posed in online lecture 2. Let $n \geq 2$ be an integer, and let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \{x \in \mathbb{Z} : 0 \leq x \leq n-1\}$. How to define operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ so that the following properties hold?

(i) $x \oplus y = x + y$ whenever $0 \leq x + y \leq n - 1$ and $x \odot y = xy$ whenever $0 \leq xy \leq n - 1$ (where the sum and the product on the right-hand sides are the usual addition and multiplication).

(ii) $\mathbb{Z}_n$ with operations $\oplus$ and $\odot$ is a commutative ring with 1.

In Lecture 2 this problem is considered for $n = 3$, where it is shown that there is at most one way to define such operations, and the only formulas for $\oplus$ and $\odot$ that could possibly work are given below: $0 \oplus x = x \oplus 0 = 0$ for all x, $1 \oplus 1 = 2$, $1 \oplus 2 = 2 \oplus 1 = 0$, $2 \oplus 2 = 1$; $0 \odot x = x \odot 0 = 0$ for all x, $1 \odot x = x \odot 1 = x$ for all x, $2 \odot 2 = 1$. We will show later that $\oplus$ and $\odot$ defined in this way do satisfy conditions (i) and (ii), but so far we do not have tools to do it in an elegant way.

(a) Solve the same problem for $n = 4$ and for $n = 5$, that is, show that there is at most one way to define $\oplus$ and $\odot$ so that (i) and (ii) hold. Present your answer in the form of multiplication and addition tables, but make sure to explain how you obtained your answer (include all computations).

(b) Assume without proof that the formulas you found in (a) do satisfy (i) and (ii). Use the multiplication table to determine whether $\mathbb{Z}_4$ is a field (with respect to those operations) and whether $\mathbb{Z}_5$ is a field. Justify your answer.