Fall 2018, Math 320: Week 5 Problem Set
Due: Tuesday, October 2nd, 2018
Properties of Rings

Discussion problems. The problems below should be completed in class.

(D1) *The ring structure of* $\mathbb{Z}_n$. The goal of this problem is to determine which elements of $\mathbb{Z}_n$ are zero-divisors, which are units, and which are neither.

(a) Compare your answers to problem (P1). Then, find all zero divisors in $\mathbb{Z}_4$, $\mathbb{Z}_5$, and $\mathbb{Z}_6$.

(b) Prove that if $m, n \geq 2$, then $\mathbb{Z}_{mn}$ is not an integral domain.

(c) Suppose p is prime. Prove that $\mathbb{Z}_p$ is an integral domain. Hint: use the fact that if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

(d) Multiply each element of $\mathbb{Z}_7$ by $[4]_7$ (i.e. find $[0]_7 \cdot [4]_7$, then $[1]_7 \cdot [4]_7$, and so forth). Do the same with $[5]_7$. What do you notice about which elements of $\mathbb{Z}_7$ appear?

(e) Multiply every element of $\mathbb{Z}_{11}$ by $[3]_{11}$. Which elements of $\mathbb{Z}_{11}$ are obtained? Hint: you may want to divide and conquer within your group!

(f) Suppose p is prime. Find and correct the error in the following proof that $\mathbb{Z}_p$ is a field.

Proof. Fix an arbitrary $a \in \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is finite, let $a_1, a_2, \ldots, a_p$ denote the complete list of distinct elements of $\mathbb{Z}_p$. We must find k so that $a_k \cdot a = [1]_p$. Consider the list

$$a_1 \cdot a, \quad a_2 \cdot a, \quad \ldots, \quad a_p \cdot a.$$

We claim these elements are all distinct (indeed, since $\mathbb{Z}_p$ is an integral domain, if $a_i \cdot a = a_j \cdot a$, then cancelling the a's yields $a_i = a_j$). This means every element of $\mathbb{Z}_p$ appears somewhere in the list. In particular, $[1]_p$ appears somewhere in the list, meaning for some k, we have $a_k \cdot a = [1]_p$. □

(g) Look carefully at the proof in part (e). What properties of $\mathbb{Z}_p$ were used in the proof? Use this to complete the following (much more general) result.

Theorem (Theorem 3.9)**.** *Suppose R is a integral domain. If* __________________, *then R is a field.*

(h) Characterize (in terms of n) when $\mathbb{Z}_n$ is a field, when $\mathbb{Z}_n$ is an integral domain but not a field, and when $\mathbb{Z}_n$ is neither an integral domain nor a field. State your characterization formally (as a theorem), and box it 3 times.

(D2) *Ring arithmetic.* Suppose $(R, +, \cdot)$ is a ring. Prove each of the following statements. Identify each ring axiom you use, and try to only use one axiom (or theorem) in each step.

(a) For every $a \in R$, $-(-a) = a$.

(b) For every $a, b \in R$, $(-a)(-b) = ab$.

(c) For every $a, b \in R$, $-(a + b) = (-a) + (-b)$.

(d) For every $a, b \in R$, $-(a - b) = (-a) + b$.

(e) If R has an identity $1_R \in R$, then for every $a \in R$, $(-1)a = -a$.

(f) If $a, b \in R$ are units, then ab is a unit.

(g) If $a, b \in R$ with a and ab both units, then b is a unit.

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Suppose $(R, +, \cdot)$ is a ring. Prove each of the following statements. Identify each ring axiom you use, and try to only use one axiom (or theorem) in each step.

(a) For any $a, b, c, d \in R$, $a - b = c - d$ if and only if $a + d = b + c$.

(b) If $a, b \in R$ are both units, then ab and a^{-1} are units as well.

(c) If R is commutative, $a, b \in R$ are zero divisors and $ab \neq 0_R$, then ab is a zero divisor.

(R2) Suppose R is an integral domain. Prove that R is commutative if and only if for every $a, b \in R$, $(ab)^2 = a^2b^2$ holds.

(R3) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If R is a ring and $a, b \in R$ are zero divisors, then $a + b$ is a zero divisor.

(b) If R is a ring and $a, b \in R$ are units, then $a + b$ is a unit.

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) Fix two rings R_1 and R_2.

(a) Characterize the units of $R_1 \times R_2$ in terms of the units of R_1 and R_2.

(b) Characterize the zero divisors of $R_1 \times R_2$ in terms of the zero divisors of R_1 and R_2.

(S2) Fix a **commutative** ring R. An element $r \in R$ is *nilpotent* if $r^n = 0$ for some $n \geq 1$.

(a) Prove that if $a, b \in R$ are nilpotent, then ab is nilpotent.

(b) Prove that if $a, b \in R$ are nilpotent, then $a + b$ is nilpotent.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Prove there is exactly one way to fill the addition and multiplication tables for a 4-element field $F = \{0_F, 1_F, a, b\}$, and give the operation tables.

Hint: read the solution to last week's challenge problem!