

Homework #1. Due Thursday, January 22nd, in class

Reading:

1. For this assignment: Section 2.1 and 2.2 + class notes (Lectures 1-2).
2. For next week's classes: Sections 2.2 and 2.3.

Problems:

Problem 1: Let R be a commutative ring with 1. Prove the following equalities using only the ring axioms and results proved or stated in class or in the book (2.1).

- (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: Many of these equalities can be proved similarly to Theorem 2.2 from the book using the cancellation law (Lemma 2.3). Note that while Theorem 2.2 formally deals with integers, its proof clearly applies to arbitrary commutative rings with 1. 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 class, 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: Recall that in class we already checked multiplication axioms (M0)-(M3), so what is left are 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: In Lecture 2, we posed the following question. Let $n \geq 2$ be an integer, and let $\mathbb{Z}_n = \{0, 1, \dots, n-1\} = \{x \in \mathbb{Z} : 0 \leq x \leq n-1\}$. 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.

We considered this problem in class for $n = 3$ and showed 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.

Problem 6: Prove by induction that the following equalities hold for any $n \in \mathbb{N}$:

- (a) $1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$
- (b) $a + ar + ar^2 + \dots + ar^{n-1} = a \frac{1-r^n}{1-r}$ where $a, r \in \mathbb{R}$ and $r \neq 1$