

Homework #5. Due on Thursday, February 25th, in class

Reading:

1. For this assignment: Online lectures 8 and 9, [Gilbert, §1.7, 2.6] and [Pinter, §12].
2. For next week's classes: Online lectures 10 and 11, [Gilbert, §3.1, 3.2] and [Pinter, §3, 4].

Problems:

Problem 1: Let A be a set and \sim an equivalence relation on A . Recall that for $a \in A$ we denote by $[a]$ its equivalence class. Prove that for any $a, b \in A$ either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Extended hint: The problem can be reformulated as follows: if $a, b \in A$ are such that $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$ (make sure you understand why this is indeed a reformulation). If $[a] \cap [b] \neq \emptyset$, there exists $c \in A$ such that $c \in [a]$ and $c \in [b]$. Use the definitions of equivalence relation and equivalence class to show that $[a] \subseteq [b]$, that is, every element of $[a]$ is also an element of $[b]$. Then by a similar argument show that $[b] \subseteq [a]$ and finally conclude that $[a] = [b]$.

Problem 2: Define the relation \sim on \mathbb{Z} as follows: $x \sim y$ if and only if $x^2 + y^2$ is even.

- (a) Prove that \sim is an equivalence relation (check 3 conditions)
- (b) Describe the equivalence classes with respect to \sim . State the number of equivalence classes, and describe all elements in each class.

Problem 3: Compute the multiplication table for the ring \mathbb{Z}_7 , use it to prove that \mathbb{Z}_7 is a field and find inverses of all nonzero elements.

Problem 4: Prove that the distributivity axioms (D1) and (D2) hold in \mathbb{Z}_n .

Problem 5: Let R be a commutative ring with 1.

- (a) An element $a \in R$ is called *invertible* if there exists $b \in R$ such that $ab = ba = 1$
- (b) An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there exists NONZERO $b \in R$ such that $ab = 0$. For instance, $[2]$ is a zero divisor in \mathbb{Z}_6 since $[2] \neq [0]$ and $[3] \neq [0]$ but $[2] \cdot [3] = [6] = [0]$ (this calculation shows that $[3]$ is also a zero divisor).

Prove that no element of R can be both invertible and a zero divisor. **Hint:** This is very similar to Problem 2 in Homework#1.

Problem 6: Do each of the following for $n = 8$ AND $n = 10$.

- (a) Compute the multiplication table in \mathbb{Z}_n
- (b) Use the multiplication table to find all invertible elements of \mathbb{Z}_n .
Check your answer using Theorem 9.1 from online Lecture 9.
- (c) Use the multiplication table to find all zero divisors of \mathbb{Z}_n
- (d) Compare your answers in (b) in (c) to each other (do this separately for $n = 8$ and $n = 10$)? How are they related? Make a conjecture about the relationship between invertible elements and zero divisors in \mathbb{Z}_n .

Problem 7: Let $n \geq 2$ be an integer. Prove that \mathbb{Z}_n has zero divisors if and only if n is non-prime. **Hint:** The forward direction (\Rightarrow) (which is best proved by contrapositive) follows directly from Problem 5 and Corollary 9.2. For the backward direction (\Leftarrow) you may want to start with $n = 6$ (in which case zero divisors are exhibited in the computation from the statement of Problem 5) and then generalize to arbitrary non-prime n .

Problem 8: Let us say that an integer $n \geq 2$ is *bad* if there exists an element $[a] \in \mathbb{Z}_n$ such that $[a] \neq [0]$ but $[a]^2 = [0]$. For instance, $n = 4$ is bad since $[2]$ is a nonzero element of \mathbb{Z}_4 , but $[2]^2 = [2^2] = [4] = [0]$.

- (a) For each $2 \leq n \leq 18$ determine whether it is bad or not (do this directly by definition). If n is bad, specify an explicit a such that $[a] \neq [0]$ but $[a]^2 = [0]$. You can save a lot of time by observing that if $[a] \neq [0]$, but $[a]^2 = [0]$, then $[a]$ is a zero divisor, hence not invertible (by Problem 6), so you only need to test whether $[a]^2 = [0]$ for non-invertible elements $[a] \in \mathbb{Z}_n$.
- (b) Based on your answer in (a), make a conjecture about which integers are bad. **Hint:** The conjecture should refer to prime factorization of n .
- (c) (bonus) Now prove the conjecture from (b).