Homework 3, Math 401

due on February 3, 2020

Before you start, please read the syllabus carefully.

We define $\gcd(m, n)$ to be the unique positive integer satisfying: 1) $d|m, n$ implies that $d|\gcd(m, n)$; 2) $\gcd(m, n)|m, n$.

1. Prove that the uniqueness of $\gcd(m, n)$ follows from the definition of $\gcd(m, n)$.

2. Prove that for any two integers m, n (not necessarily positive), $\gcd(m, n) = 1$ if and only if there exist integers a and b such that $a \cdot m + b \cdot n = 1$. (Use Euclidean algorithm.)

3. Prove that a non-zero element in $\mathbb{Z}_m$ is either a unit or a zero-divisor. Deduce the number of units for $\mathbb{Z}_m$ when:

   (a) $m = p$ where p is a prime number

   (b) $m = p^r$ where p is a prime number

   (c) $m = p_1 \cdot p_2$ where $p_1 \neq p_2$ are prime numbers

4. For a general ring R, is it true that a non-zero element in R is either a unit or a zero-divisor? If yes, give a proof; if no, give a counter example.

5. Let R be an integral domain having a finite number of elements. Prove R is a field. (Ex 12 in 1.4)

6. Let R be a ring (not necessarily commutative). Given that a, b and $a+b \in R$ are all units, prove that $a^{-1} + b^{-1}$ is a unit.

7. Consider the polynomial rings with coefficient in $\mathbb{Z}_5$. Do the division algorithms (i.e. find $q(x)$ and $r(x)$ in $\mathbb{Z}_5[x]$ such that $f(x) = g(x)q(x) + r(x)$):

   (a) $f(x) = 3x^3 - 2x^2 + 1, \qquad g(x) = 2x + 1;$

   (b) $f(x) = x^5 - 1 \qquad g(x) = x - 1.$

8. Consider the polynomial rings with coefficient in $\mathbb{Q}$. Do the division algorithms:

   (a) $f(x) = 3x^3 - 2x^2 + 1, \qquad g(x) = 2x + 1;$

   (b) $f(x) = x^5 - 1, \qquad g(x) = x - 1.$

   (*): Can you see from this exercise why we do not do division algorithm for $\mathbb{Z}[x]$?

9. Prove that $\mathbb{Q}[\sqrt{2}]$ is a field. The set contains all elements in the form of $a + b\sqrt{2}$ where a and b are in $\mathbb{Q}$. The addition and multiplication is defined as the same addition and multiplication in real numbers.

10. Given two ideals $I = \langle f(x) \rangle$ and $J = \langle g(x) \rangle$, porve that $I \subset J$ if and only if $g(x)|f(x)$.

11. Find all possible ring homomorphisms from A to B:

    (a) $A = \mathbb{Z}_{10}, \qquad B = \mathbb{Z}$

    (b) $A = \mathbb{Z}_{10}, \qquad B = \mathbb{Z}_5$

    (c) $A = \mathbb{Z}_{10}, \qquad B = \mathbb{Z}_3$

12. Prove that if I and J are ideals, then $I \cap J$ and $I + J$ are both ideals. Here $I \cap J := \{r \in R \mid r \in I, r \in J\}$, $I + J := \{r \in R \mid \exists a \in I, b \in J \text{ such that } r = a + b\}$.