3/10/17 Spring 2017, Intro to Modern Algebra II Test II Solutions Sitaraman

EACH PROBLEM 20 POINTS. ANSWER AS MANY AS YOU CAN.

1.Show that a finite integral domain is a field.

Solution: This was done in class. Also a homework problem.

2. Let R be a commutative ring. Show that the subset generated by two elements $a, b \in R$ given by $I = \{ra + sb \mid r, s \in R\}$ is an ideal. Such an ideal is also denoted by (a, b). Given $a, b \in \mathbb{Z}$ prove that this is just the ideal generated by the GCD (a, b).

Solution: This is basically theorem 4.5.7.

3. Let $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers.

(a) Produce a 1-1 surjective ring homomorphism from $R/(1 + i)$ to $\mathbb{Z}/2\mathbb{Z}$, the field of two elements.

(b) Conclude that $(1 + i)$ is a maximal ideal in R.

Solution: a) We have $(1 + i)(1 - i) = 2$. So we have $2 \in (1 + i)$. From this we get $i \equiv -1 \equiv -2 + 1 \equiv 1 \ mod \ (1+i)$. Given any integer a we have $a \equiv 0$ or $a \equiv 1 \ mod \ 2$ which means $a \equiv 1$ or $0 \ mod \ (1+i)$ because 2 is in $(1 + i)$.

So after reducing $a, b \ mod \ 2$ (and hence $(1 + i)$) and $i \ mod \ (1 + i)$ we get that $a + bi \equiv r \ mod \ (1 + i)$ where $r = 0$ or 1.

The map is given by $a + bi + R \mapsto r \ mod \ (1 + i)$.

This is easily shown to be a 1-1 onto ring homomorphism.

[The homomorphism part comes from the fact that addition and multiplication are preserved under congruence relation. If $a \equiv a_1$ and $b \equiv b_1$ modulo something then $a + b \equiv a_1 + b_1$ and $ab \equiv a_1 b_1$ modulo the same].

b) This follows from the theorem that the quotient ring is a field iff the ideal is maximal.

4. With R as in problem 3, let $F = R/3R$.

a) (8 points) By reducing every element in R modulo 3, show that F is a field with 9 elements.

a) (6 points) Show that $3x = 0$ for all $x \in F$.

b) (6 points) Show that $(x + y)^3 = x^3 + y^3$ for all $x, y \in F$.

Solution: Note that elements in F are the cosets $a + bi + 3R$.

a) If $a + bi \in R$ then the coset $a + bi + 3R = c + di + 3R$ where $a \equiv c \ mod \ 3$ and $b \equiv d \ mod \ 3$. Here c, d can only be one of 0,1, or 2. It is easy to see that we get nine distinct cosets this way.

b) There is more than one way to prove this. One is to say that if $x \in F$ then $3x = 3R$ because for any coset $x = a + bi + 3R$ we have $3x = 3a + 3bi + 3R = 3R$. So in $F = R/3R, 3x = 0$. Another way is to see that the order of F is 3^2 and since any finite field is of order p^n for a prime p such that $px = 0$ for all elements in that field, here we must have $3x = 0$ for all $x \in F$.

c) This is easily seen by expanding $(x + y)^3$ as $x^3 + 3x^2y + 3xy^2 + 3y^3$ and then using (b).

5. Give on example for each. Explain how they satisfy each of the conditions given.

a) (10 points) A polynomial in $\mathbb{Q}[x]$ that has no roots in $\mathbb{Q}$ but is reducible in $\mathbb{Q}[x]$.

b) (10 points) A proper subring of $\mathbb{Q}$ that is bigger than $\mathbb{Z}$.

Solution:

a) $x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$.

b) We can use the example 3 in 4.3 given in the book. In fact there are two subrings there, one called R that is composed of all fractions with denominator not divisible by a fixed prime number p. The other subring (which is actually an ideal of R) composed of all fractions in R whose numerator is divisible by that prime number. We will denote it as pR.

6. Prove the following.

a) (10 points) Every subring of $\mathbb{Z}$ is also an ideal.

b) (10 points) A proper, nontrivial subring of $\mathbb{Q}$ cannot be an ideal of $\mathbb{Q}$. What are the ideals of $\mathbb{Q}$?

Solution:

a) Every subring is also a subgroup under addition, hence a cyclic subgroup as well, of the form $n\mathbb{Z}$. But as we know, these are all the ideals of $\mathbb{Z}$ since it is a principal ideal domain.

b) $\mathbb{Z}, pR$ are proper nontrivial subrings of $\mathbb{Q}$ and it is easy to see why they are not ideals. The ideals of $\mathbb{Q}$ are just itself and (0) because it is a field.