Homework

Frederick Robinson

6 February 2010

Contents

1 Chapter 9 Section 1

1.1 Problem 4

1.1.1 Question

Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal idea.

1.1.2 Answer

I claim that (x) is a prime ideal in $\mathbb{Q}[x, y]$.

Proof. Let $ab \in (x)$ be the product of two elements in $\mathbb{Q}[x, y]$. We wish to show that either $a \in (x)$ or $b \in (x)$. Since $ab \in (x)$ we know that each term of ab has at least one x. Assume towards a contradiction that neither $a \in (x)$ nor $b \in (x)$. Then each of a and b contain at least one term which has no x. Hence, their product contains a terms which is the product of these terms and contains no x. Contradiction. □

I claim that (x, y) is a prime ideal in $\mathbb{Q}[x, y]$.

Proof. Let $ab \in (x, y)$ be the product of two elements in $\mathbb{Q}[x, y]$. We wish to show that either $a \in (x, y)$ or $b \in (x, y)$. Since $ab \in (x, y)$ we know that each term of this product must contain an x or a y. Assume towards a contradiction that $a \notin (x, y)$ and $b \notin (x, y)$. Then neither has the property that each term contains an x or a y. Thus each has at least one term which contains neither xs nor ys. However, the product of such a term contains neither xs nor ys. Contradiction. □

I claim that (x, y) is a maximal ideal.

Proof. Suppose that (x, y) is not a maximal ideal, then there exists some other ideal say I such that $(x, y) \subsetneq I \subsetneq \mathbb{Q}[x, y]$. Since every element of $\mathbb{Q}[x, y]$ which contains only terms with x and y is contained in (x, y) it must be that I contains at least one element say k such that k has at least one term with neither xs nor ys. However $I \subset (x, y, k) = \mathbb{Q}[x, y]$. In particular since (x, y, k) is an ideal it must be that it is closed under addition. Furthermore there exists an element of (x, y) say l whose terms containing x and y are the same as those of k but with opposite sign since (x, y) contains each element of $\mathbb{Q}[x, y]$ whose terms each have x and y. This means that $k + l \in (x, y, k) = c$ for some constant term c. Then, since an ideal must be closed under multiplication by elements of the ring and since $\mathbb{Q}$ is closed under multiplicative inverse $1 \in (x, y, k) \Rightarrow (x, y, k) = \mathbb{Q}[x, y]$ □

I claim that (x) is not a maximal ideal.

Proof. First observe that $(x) \subset (x, y)$ by definition of finitely generated ideals. Moreover I claim that $(x) \neq (x, y)$. In particular though y is an element of the latter ideal it is not in the former. □

1.2 Problem 5

1.2.1 Question

Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.

1.2.2 Answer

I claim that (x, y) is a prime ideal in $\mathbb{Z}[x, y]$.

Proof. Let $ab \in (x, y)$ be the product of two elements in $\mathbb{Z}[x, y]$. We wish to show that either $a \in (x, y)$ or $b \in (x, y)$. Since $ab \in (x, y)$ we know that each term of this product must contain an x or a y. Assume towards a contradiction that $a \notin (x, y)$ and $b \notin (x, y)$. Then neither has the property that each term contains an x or a y. Thus each has at least one term which contains neither xs nor ys. However, the product of such a term contains neither xs nor ys. Contradiction. □

I claim that $(2, x, y)$ is a prime ideal in $\mathbb{Z}[x, y]$.

Proof. Let $ab \in (2, x, y)$ be the product of two elements in $\mathbb{Z}[x, y]$. We wish to show that either $a \in (2, x, y)$ or $b \in (2, x, y)$. Since $ab \in (x, y)$ we know that each term of this product must contain an x or a y except for possibly a constant term which must be a multiple of 2 if it is present. Assume towards a contradiction that $a \notin (x, y)$ and $b \notin (x, y)$. Then neither has the property that each term contains an x or a y except for a constant term which must be a multiple of 2 if present. Thus each has a constant term which is not a multiple of 2. However, the product of these terms is not 2 since in $\mathbb{Z}$ the only numbers whose product is a multiple of 2 are themselves multiples of 2 (or 1, but if this is the case then the other must be a multiple of 2). Contradiction. $\square$

I claim that $(2, x, y)$ is a maximal ideal in $\mathbb{Z}[x, y]$.

Proof. Suppose towards a contradiction that there exists some ideal say I such that $(2, x, y) \subsetneq I \subsetneq \mathbb{Z}[x, y]$. In particular I must contain some element of $\mathbb{Z}[x, y]$ which is not in $(2, x, y)$. Since each element of $\mathbb{Z}$ which has no constant term is in $(2, x, y)$, our new element of I must have a constant term. Also, since each member of $\mathbb{Z}[x, y]$ whose constant term is a multiple of 2 is a member of $(2, x, y)$ the constant term of our new element must not be a multiple of 2. So, we have established that there exists $k \in I$ such that k has a constant term which is of the form $k = 2n + 1$ for some $n \in \mathbb{Z}$. Now, since I is a superset of $(2, x, y)$ and must be closed under addition (by definition of an ideal) it must also contain just k since in $(2, x, y)$ there is an element whose nonconstant terms are the same as those of k but with opposite sign. Similarly by closure under addition $1 \in I$ since $-2n \in (2, x, y) \Rightarrow 2n + 1 - 2n = 1 \in I$. Thus, $I = \mathbb{Z}[x, y]$. $\square$

I claim that (x, y) is not a maximal ideal.

Proof. By definition of finitely generated ideals we have that $(x, y) \subset (2, x, y)$. Furthermore since in particular $2 \in (2, x, y)$ but $2 \notin (x, y)$ we have $(x, y) \neq$

$(2, x, y)$. Thus, $(x, y) \subset (2, x, y) \subset \mathbb{Z}[x, y]$ and (x, y) is not a maximal ideal.

$\square$

1.3 Problem 6

1.3.1 Question

Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.

1.3.2 Answer

I claim that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.

Proof. In particular there exist no element k such that $(k) = (x, y)$. For suppose towards a contradiction that there exists such a k. Then, each member of (x, y) may be written as a product of k and a member of $\mathbb{Q}[x, y]$. In particular since $x, y \in (x, y)$ we have that $x = k \cdot l$ and $y = k \cdot m$. However this implies that $k \in \mathbb{Q}$, but (x, y) contains no constant polynomials. Contradiction. $\square$

2 Chapter 9 Section 2

2.1 Problem 1

2.1.1 Question

Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n-1$ such that $\overline{g(x)} = \overline{g_0(x)}$ (equivalently, the elements $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ are a *basis* of the vector space $F[x]/(f(x))$ over F – in particular, the dimension of this space is n). [Use the Division Algorithm.]

2.1.2 Answer

I claim that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n-1$ such that $\overline{g(x)} = \overline{g_0(x)}$

Proof. Let $g(x)$ be a polynomial over F of degree $m > n$ and maximal coefficient is z. Then, if we take the sum $g(x) - zx^{m-n}f(x)$ we will get an element of the same equivalence class mod $f(x)$ as $g(x)$ since we are just subtracting by a multiple of $f(x)$. Since we can repeat this as long as the degree of $g(x)$ is greater than or equal to that of $f(x)$ we can use this method to generate a representative $g_0(x)$ of $\overline{g(x)}$ which has degree $\leq n-1$.

Moreover $g_0(x)$ is the unique such polynomial with degree $\leq n-1$ for any two polynomials $h(x)$ and $j(x)$ whose degree are is less than that of $f(x)$ are distinct mod $f(x)$. Suppose not, then there would exist an element

$l(x) \in (f(x))$ such that $l(x) + j(x) = h(x)$ However each potential $l(x)$ can be written as $f(x)t(x) = l(x)$ for some nonzero $t(x) \in F[x]$. So we get $f(x)t(x) + j(x) = h(x)$. However, any product of $f(x)$ with some other nonzero polynomial has degree at least that of $f(x)$ but then $N(f(x)t(x)) \geq n$ whereas $N(h(x)) \leq n - 1$. Contradiction. $\square$

2.2 Problem 2

2.2.1 Question

Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements. [Use the preceding exercise.]

2.2.2 Answer

I claim that if F is a finite field of order q and $f(x)$ a polynomial in $F[x]$ of degree $n \geq 1$ then $F[x]/(f(x))$ has q^n elements.

Proof. Let $g(x) \in F[x]$. By the previous exercise $\overline{g(x)}$ has a unique representative in $F[x]/(f(x))$ with degree $\leq n - 1$. There are q^n polynomials of degree strictly less than n. Each x^n term has one of the q members of F as its coefficient. Since there are q^n such elements there are q^n distinct equivalence classes in $F[x]/(f(x))$. Each equivalence class corresponding to a given polynomial of degree $\leq n - 1$ is nonempty since in particular it contains the representative polynomial. $\square$

2.3 Problem 7

2.3.1 Question

Determine all the ideals of the ring $\mathbb{Z}[x]/(2, x^3+1)$.

2.3.2 Answer

By an isomorphism theorem we can write

$$\mathbb{Z}[x]/(2, x^3+1) \cong (\mathbb{Z}[x]/2)/((2, x^3+1)/(2)) \cong \mathbb{Z}/2\mathbb{Z}[x]/(x^3+1)$$

$$\cong \mathbb{Z}/2\mathbb{Z}/((x+1)(x^2+x+1))$$

and by Proposition 16 this is just

$$\cong \mathbb{Z}/2\mathbb{Z}/(x+1) \times \mathbb{Z}/2\mathbb{Z}/(x^2+x+1)$$

So the ideals of this ring are just multiples of $\cong \mathbb{Z}/2\mathbb{Z}/(x+1)$ and $\mathbb{Z}/2\mathbb{Z}/(x^2+x+1)$

2.4 Problem 8

2.4.1 Question

Determine the greatest common divisor of $a(x) = x^3 - 2$ and $b(x) = x+1$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.

2.4.2 Answer

Both $a(x)$ and $b(x)$ are irreducible. The former is irreducible since it has no roots in $\mathbb{Q}$, and the latter because it has no constant rational divisors. Thus, by proposition 13 page 287 their greatest common factor is just 1. We can write 1 as a linear combination in $\mathbb{Q}[x]$ as

$$1 = \frac{1}{3}(x+1)(x^2 - x + 1) - 1(x^3 - 2)$$

3 Chapter 9 Section 4

3.1 Problem 1

3.1.1 Question

Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime.

1. $x^2 + x + 1$ in $\mathbb{F}_2[x]$.

2. $x^3 + x + 1$ in $\mathbb{F}_3[x]$.

3. $x^4 + 1$ in $\mathbb{F}_5[x]$.

4. $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

3.1.2 Answer

1. $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ since it has no roots and its coeffients have no multiple in common.

2. $x^3 + x + 1 = (x - 1)(x^2 + x + 2)$ in $\mathbb{F}_3[x]$.

3. $x^4 + 1$ has no roots in $\mathbb{F}_5[x]$. Thus any factorization of $x^4 + 1$ must be as a product of order 2 terms. Moreover since the only pairs of elements of $\mathbb{F}_5$ whose product is 1 are 2,3 and 4,4 and 1,1 there are but a few possibilities for factorizations. Checking each as in the next part reveals that there are no such factorizations.

4. $x^4 + 10x^2 + 1$ has no roots in $\mathbb{Z}[x]$ since it is monic and by Proposition 11, $1 + 10 + 1 = 12 \neq 0$ implies it has no roots. Thus, if it is reducible it must be as a product of order 2 terms. However, this being the case each such term must be of the form $\pm x^2 + ax \pm 1$ for some a since in $\mathbb{Z}$ the only numbers whose product is 1 are 1 and -1. Thus we must have a product of one of the following forms:

$$1 + ax + bx - 2x^2 + abx^2 - ax^3 - bx^3 + x^4$$

$$1 - ax - bx - 2x^2 + abx^2 + ax^3 + bx^3 + x^4$$

$$1 - ax - bx + 2x^2 + abx^2 - ax^3 - bx^3 + x^4$$

$$1 + ax + bx + 2x^2 + abx^2 + ax^3 + bx^3 + x^4$$

of course up to change in a and b the only of these which are unique are

$$1 - ax - bx - 2x^2 + abx^2 + ax^3 + bx^3 + x^4$$

and

$$1 + ax + bx + 2x^2 + abx^2 + ax^3 + bx^3 + x^4$$

If the former were the case then we would have $ab - 2 = 10$ and $-a - b = 0$ and $a + b = 0$. This is a contradiction however since the $-a - b = 0 \Rightarrow a = b = 0$ but $0 - 2 \neq 10$. If the latter were the case we would get a contradiction as well since we would have $a + b = 0$ and $2 + ab = 10$ and $a + b = 0$. The first equation implies that $ab \leq 0$ but this is inconsistent with the second equation. Thus $x^4 + 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$

4 Chapter 9 Section 5

4.1 Problem 5

4.1.1 Question

Let φ denote Euler's φ-function. Prove the identity $\sum_{d|n} \varphi(d) = n$, where the sum is extended over all the divisors d of n. [First observe that the identity is valid when $n = p^m$ is the power of a prime p since the sum telescopes. Write $n = p^m n'$ where p does not divide n'. Prove that $\sum_{d|n} \varphi(d) = \sum_{d''|p^m} \varphi(d'') \sum_{d'|n'} \varphi(d')$ by multiplying out the right hand side and using the multiplicativity $\varphi(ab) = \varphi(a)\varphi(b)$ when a and b are relatively prime. Use induction to complete the proof. This problem may be done alternatively by letting Z be the cyclic group of order n and showing that because Z contains a unique subgroup of order d for each d dividing n, the number of elements of Z of order d is $\varphi(d)$. Then $|Z|$ is the sum of $\varphi(d)$ as d runs over all divisors of n.]

4.1.2 Answer

Let Z be the cyclic group of order n. Z contains a unique subgroup of order d for each d which divides n by the Fundamental Theorem of Cyclic Groups. In particular if $Z = \langle x \rangle$ these subgroups are given by the powers of $x^{n/d}$. Since the members of such a subgroups whose order is d is just $\varphi(d)$ and an element of a group can have order d if and only if it is a member of a cyclic subgroup of order d we see that the number of elements in Z whose order is d is given by $\varphi(d)$. Since the members of a cyclic group are all of some finite order less than that of the group we see in particular that $|Z| = n = \sum_{d|n} \varphi(d)$ as claimed.