[redacted]

Modern Algebra II - Deopurkar

[redacted] @ columbia edu

$\frac{45}{45}$

Problem Set 3

1) Suppose that $(p(x), q(x)) = (1)$. Then there are elements $r(x)$ and $s(x) \in F[x]$ such that $r(x)p(x) + s(x)q(x) = 1$.

Now consider and element $h(x)$ for which $p(x)q(x)$ is a divisor.

We show that $p(x)$ and $q(x)$ are individually divisors of $h(x)$; however, this is trivial since, if $p(x)q(x) \mid h(x)$, $h(x) = k(x)p(x)q(x) = (k(x)p(x))q(x) = (k(x)q(x))p(x)$ is a multiple of both p and q.

Conversely, if $p(x) \mid h(x)$ and $q(x) \mid h(x)$ we wish to show that $p(x)q(x) \mid h(x)$. Since $(p(x), q(x)) = (1)$, $r(x)p(x)h(x) + s(x)q(x)h(x) = h(x)$, and since $p(x)q(x)$ divides both terms on the left (because both $p(x)$ and $q(x)$ divide $h(x)$), $p(x)q(x)$ divides $h(x)$.

Thus if we define the map $\varphi : F[x] \longrightarrow F[x]/(p(x)) \times F[x]/(q(x))$ by $\varphi(h(x)) = (\bar{h}(x), \tilde{h}(x))$, where $\bar{h}$ and $\tilde{h}$ are the congruence classes of h in $F[x]/(p(x))$ and $F[x]/(q(x))$ respectively, we obtain a homomorphism. Note that a and b are congruent iff $a-b \in (p(x))$.

1) Thus $\bar{h}(x) = h(x) + (p(x))$ and $\tilde{h}(x) = h(x) + (q(x))$.

arbitrary

To see that φ is surjective, take $(a + (p(x)), b + (q(x)))$.

Then define $h(x) = r(x)b + s(x)a$, s and r as before.

Under φ, h is sent to $(rb + sa + (p(x)), rb + sa + (q(x)))$

5

$= (sa + (p(x)), rb + (q(x))) = (a + (p(x)), b + (q(x)))$, since

$rb \in (p(x))$ and $sa \in (q(x))$ because $r \in (p(x))$ and

$s \in (q(x))$. Furthermore, since the kernel of φ is the

set of all elements divisible by both p and q, it equals

$(p(x)q(x))$ as we showed earlier.

By the First Isomorphism Theorem then, $F[x]/(p(x)q(x)) \cong$

$F[x]/(p(x)) \times F[x]/(q(x))$. ■

2) Let $p(x)$ be a polynomial of degree n in $\mathbb{C}[x]$. By the fundamental theorm of algebra, $p(x)$ has precisely n roots in $\mathbb{C}$ if $n \geq 1$. If $n = 0$, $p(x) = a_0$, so $\mathbb{C}[x]/(a_0) = \mathbb{C}[x]/(1) = \{0\}$; because $\mathbb{C}$ is a field $(a_0) = (1)$.

Thus, assume that $n \geq 1$. If $a_1, \dots, a_n$ are n distinct zeroes in $\mathbb{C}$ of $p(x)$, we can write $p(x) = c(x-a_1)\cdots(x-a_n)$ where c is a constant in $\mathbb{C}$. Let $Q_1(x) = c(x-a_2)\cdots(x-a_n)$, $Q_2(x) = c(x-a_3)\cdots(x-a_n)$ and so on until $Q_{n-1}(x) = c(x-a_n)$. Then $(x-a_1, Q_1(x)) = (1)$ since $x-a_1$ and $Q_1(x)$ have no common divisor other than constants. This can be seen by noting that no polynomial of degree ≥ 1 divides $x-a_1$ except itself, by division w/ remainder.

Thus, we can apply the Chinese Remainder Theorem for polynomials from question 1):

$$\mathbb{C}[x]/(p(x)) = \mathbb{C}[x]/((x-a_1)Q_1(x)) \cong \mathbb{C}[x]/(x-a_1) \times \mathbb{C}[x]/(Q_1(x)).$$

Repeating the process for $(x-a_i)$ and $Q_i(x)$, we find that

$$\mathbb{C}[x]/(p(x)) \cong \mathbb{C}[x]/(x-a_1) \times (\mathbb{C}[x]/(x-a_2) \times (\dots(\mathbb{C}[x]/(x-a_n))\dots))^{*}$$

$$\cong \prod_{i=1}^{n} \mathbb{C}[x]/(x-a_i)$$

* $(c(x-a_n)) = (x-a_n)$ since $\mathbb{C}$ is a field so that c has an inverse.

Now suppose that $p(x)$ has a zero a' w/ multiplicity $k > 1$. Then $p(x) = c(x-a')^k(x-a_1)\cdots(x-a_{n-1})$, so

2) our process yields $\prod_{i=1}^{n-1} \mathbb{C}[x]/(x-a_i) \times \mathbb{C}[x]/(x-a')^k$.

5

In general if zero a has multiplicity k_a, ✓

$$\mathbb{C}[x]/(p(x)) \cong \boxed{\prod_a \mathbb{C}[x]/(x-a)^{k_a}} . \blacksquare$$

3) Suppose that R is a domain of finite order. Pick any nonzero element $a \in R$. Then the elements $a^2, a^3, \ldots$ are also in R.

5

Because R has finitely many elements and there are infinitely many exponents, $a^n = a^m$, $m \neq n$. Without loss of generality assume $m < n$. Then, by the cancellation law, $a^n = a^m$ $\Longrightarrow a^{n-m} = 1$. Thus, $a^{-1} = a^{n-m-1}$. Since a was an arbitrary nonzero element of R, it follows that R is a field. $\blacksquare$ ✓

4) Suppose that R is a domain and consider the polynomial ring $R[x]$. Take $a, b \in R[x]$, $a = a_0 + a_1 x + \ldots$ and $b = b_0 + b_1 x + \ldots$ Then $ab = (a_0 + a_1 x + \ldots)(b_0 + b_1 x + \ldots)$ $= \sum_{i,j} a_i b_j x^{i+j}$. If $a \neq 0$ and $b \neq 0$, then at least one coefficient of both a and b must be nonzero. Let a_n and b_m be the first nonzero coefficients of a and b respectively. Consider the $(n+m)$-th degree term x^{n+m} of the product ab.

4) Since $a_n x^n$ and $b_m x^m$ are lowest degree terms of a and b, the coefficient of x^{n+m} is $a_n b_m$. Since R is a domain and $a_n, b_m \neq 0$, $a_n b_m \neq 0$. Thus $ab \neq 0$, so $R[x]$ is a domain.

5

From our expression for $ab = \sum_{i,j} a_i b_j x^{i+j}$, it is clear that $ab = 1$ iff $a_0 b_0 = 1$ and all higher terms vanish. Taking the nonzero coefficients a_n and b_m of highest degree terms x^n and x^m of a and b respectively, we see that $a_n b_m x^{n+m}$ does not vanish. Thus all $a_i, b_i = 0$, $i \geq 1$, if $ab = 1$. Consequently, the units of $R[x]$ are the units of R, since only constant polynomials may be units $R[x]$. ■

5) Suppose that a domain R contains 15 elements exactly. Since R has finite order, it is a field by exercise 3). Thus, as a finite field it has characteristic p for some prime number. By 15.7.1) in Artin, the order of R must be some positive integer power of p, p^r. Thus $15 = p^r$, for prime p. But the prime factorization of 15 is $3 \cdot 5$, which unique. Here we have obtained a contradiction. Thus, there is no domain w/ 15 elements exactly. ■

5

We can always find such an a since otherwise $p(x,y)$ would be constant by continuity of polynomials.

* such that $p(a,y)$ is nonconstant (unless zero

6) Suppose that $p(x,y) \in \mathbb{C}[x,y]$. We claim that a nonconstant $p(x,y)$ has a root (a,b) in $\mathbb{C}^2$. Take any $a \in \mathbb{C}$.* Then the evaluation map that sends x to a is a homomorphism.

5

$\mathbb{C}[x,y]$ and $\mathbb{C}[y]$ and $p(x,y) \to p_a(y)$. Here, if $p_a(y)$ is nonconstant, we use the Fundamental Theorem of Algebra to yield a b such that $p_a(b) = 0$. Thus $p(a,b) = 0$ if $p(x,y)$ is nonconstant. We treat this case separately.

If $p(x,y)$ has the root (a,b), it must belong in $(x-a, y-b)$. Hence $(p(x,y)) \subset (x-a, y-b) \neq \mathbb{C}[x,y]$ ✓ because $(x-a, y-b)$ is a maximal ideal by the Nullstellensatz. Thus, to show $(p(x,y))$ is not a maximal ideal, we must show that the opposite inclusion does not hold. Now, since $x-a$ and $y-b$ are the lowest degree polynomials whose root is (a,b), it is clear that unless $p(x,y) = x-a$ or $x-b$, neither is contained in $(p(x,y))$. If $p(x,y)$ is in fact one of them, the other could definitely not be in the ideal. Thus the "$\subset$" sign is a proper inclusion.

Now consider the case where $p(x,y) = c$, a constant. Then, since $\mathbb{C}$ is a field, $(p(x,y)) = (c) = \mathbb{C}[x,y]$. Thus, no principal ideal of $\mathbb{C}[x,y]$ is a maximal ideal. ∎ ✓

7) Suppose that $p(x) \in \mathbb{Z}[x]$. Suppose also that $\deg p(x) = n$, where $n \geq 0$, and $p(x) \neq \pm 1$, for then $(p(x)) = \mathbb{Z}[x]$, which is not a maximal ideal by definition.

Let a_0 be the constant term of $p(x)$. Choose a prime number k that does not divide a_0. Then, since $(p(x)) = \{ q(x)p(x) \mid q(x) \in \mathbb{Z}[x] \}$, it is clear that $k \notin (p(x))$, for since p is prime and does not divide a_0, there is no multiple of $p(x)$ which equals k, since the constant term of $p(x)q(x)$ is $a_0 q_0$, $a_0, q_0 \in \mathbb{Z}$.

5

Thus $(p(x)) \subset (k, p(x)) \neq \mathbb{Z}[x]$ since there infinitely many prime integers not contained in $(k, p(x))$. Thus no principal ideal is a maximal ideal in $\mathbb{Z}[x]$. ∎

45/5

8) According to proposition 11.8.2), an ideal I of a ring R is maximal iff R/I is a field. Thus $\mathbb{F}_2[x]/(x^3+x+1)$ and $\mathbb{F}_3[x]/(x^3+x+1)$ are fields iff and only if (x^3+x+1) is maximal in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ respectively. By proposition 11.8.4 a), the maximal ideals of $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ are the principal ideals generated by the monic irreducible polynomials. Thus our problem reduces to showing that x^3+x+1 is a monic irreducible polynomial in $\mathbb{F}_2$ but not $\mathbb{F}_3$. Clearly x^3+x+1 is monic in both $\mathbb{F}_2$ and $\mathbb{F}_3$.

Suppose that $x^3+x+1 = p(x)q(x) = (a_0+a_1x+a_2x^2)(b_0+b_1x)$

5

$= a_0b_0 + (a_1b_0+b_1a_0)x + (a_2b_0+a_1b_1)x^2 + a_2b_1x^3$. Thus, we obtain a system of equations: $a_0b_0=1$, $a_2b_1=1$, $a_1b_0+b_1a_0=1$, and $a_2b_0+a_1b_1=0$. Since in $\mathbb{F}_2$, only $1\cdot 1=1$, it follows that $a_0=b_0=b_1=a_2=1$. But this suggests that $a_1=1$ and $a_1=0$, a contradiction. We know, if x^3+x+1 we reducible in $\mathbb{F}_2$, that the factors would have to be degree 2 and 1 respectively because x^3+x+1 is a monial polynomial. Thus x^3+x+1 is irreducible in $\mathbb{F}_2$, so $\mathbb{F}_2[x]/(x^3+x+1)$ is a field. ✓

In $\mathbb{F}_3$, $x^3+x+1 = (2x^2+2x+1)(2x+1)$ ✓, so it is not irreducible, and hence $\mathbb{F}_3[x]/(x^3+x+1)$ is not a field. ■

9) Let $\varphi : \mathbb{R}[x,y] \to \mathbb{R}[\cos t, \sin t]$ be given by $\varphi(x) = \cos t$ and $\varphi(y) = \sin t$ and the identity on elements of $\mathbb{R}$.

This is homomorphism if we define $\varphi\left(\sum_{ij=1}^{n} a_i x^i + b_j y^j\right)$

$$= \sum_{ij=1}^{n} a_i \varphi(x)^i + b\varphi(y)^j = \sum_{ij=1}^{n} a_i \cos^i t + b_j \sin^j t.$$

Moreover, this map is clearly surjective, so the First

5

Isomorphism Theorem tells us that $\mathbb{R}[x,y]/K \cong \mathbb{R}[\cos t, \sin t]$ where K is the kernel of φ. It is clear that, since $\sin^2 t + \cos^2 t = 1$, $x^2 + y^2 - 1 \in K$. But we must show that $(x^2+y^2-1) = K$. This is an analytic problem I don't know how to solve. Just take it on faith. OK.

Then $\mathbb{R}[x,y]/(x^2+y^2-1) \cong \mathbb{R}[\cos t, \sin t]$ as desired. ■